Configurer et dépanner SSO sur Cisco Unified Communications Manager (CUCM)

Contenu

Introduction

Ce document décrit la fonctionnalité d'authentification unique (SSO) dans Cisco Unified Communications Manager (CUCM), les étapes de configuration, des conseils de dépannage, des exemples d'analyse de journal et des ressources pour obtenir des informations supplémentaires.

Conditions préalables

Conditions requises

Afin de comprendre ce document, Cisco recommande de connaître quelques termes SSO :

- Security Assertion Markup Language (SAML) : norme ouverte permettant d'échanger des données d'authentification et d'autorisation entre les parties
- Fournisseur de services (SP) : le SP est l'entité qui héberge le service. Dans ce document, CUCM est le fournisseur de services
- Fournisseur d'identité (IdP) : l'IdP est l'entité qui authentifie les informations d'identification du client. L'authentification est entièrement transparente pour le SP, de sorte que les informations d'identification peuvent être une carte à puce, un nom d'utilisateur/mot de passe, etc. Une fois que le fournisseur d'identité authentifie les informations d'identification d'un client, il génère une assertion, l'envoie au client et redirige le client vers le fournisseur de services
- Assertions : élément d'information sensible au temps que le fournisseur d'identité génère après l'authentification réussie d'un utilisateur. L'objectif de cette affirmation est de fournir des informations sur l'utilisateur authentifié au SP
- Liaisons : définit la méthode de transport utilisée pour remettre les messages du protocole SAML entre les entités. Les produits Cisco Unified Communications utilisent le protocole HTTP
- Profils : contraintes et combinaisons prédéfinies de contenu de message SAML (assertions, protocoles, liaisons) qui permettent de réaliser un cas d'utilisation spécifique. Cette formation est axée sur le profil d'authentification unique du navigateur Web, qui est la méthode utilisée par CUCM
- Métadonnées : ensemble d'informations de configuration échangées entre les parties. Contient des informations telles que les liaisons SAML prises en charge, les rôles opérationnels tels que IdP ou SP, les attributs d'identificateur pris en charge, les informations d'identificateur et les informations de certificat utilisées pour signer et chiffrer la demande ou la réponse.

Components Used

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

L'objectif de l'authentification unique est de permettre aux utilisateurs et aux administrateurs d'accéder à plusieurs applications de collaboration Cisco sans avoir besoin d'authentifications distinctes pour chacune d'elles. L'activation de l'authentification unique présente plusieurs avantages :

- Elle améliore la productivité, car les utilisateurs n'ont pas besoin de saisir à nouveau des informations d'identification pour la même identité sur différents produits.
- Il transfère l'authentification de votre système qui héberge les applications vers un système tiers. Vous créez un cercle de confiance entre un fournisseur d'identité et un fournisseur de

services qui lui permet d'authentifier les utilisateurs au nom du fournisseur de services.
- Il fournit un cryptage pour protéger les informations d'authentification transmises entre le fournisseur d'identité, le fournisseur de services et l'utilisateur.SSO masque également les messages d'authentification transmis entre le fournisseur d'identité et le fournisseur de services à partir de toute partie externe.
- Elle peut réduire les coûts car moins d'appels sont passés au centre d'assistance pour réinitialiser les mots de passe.

Cercle de confiance

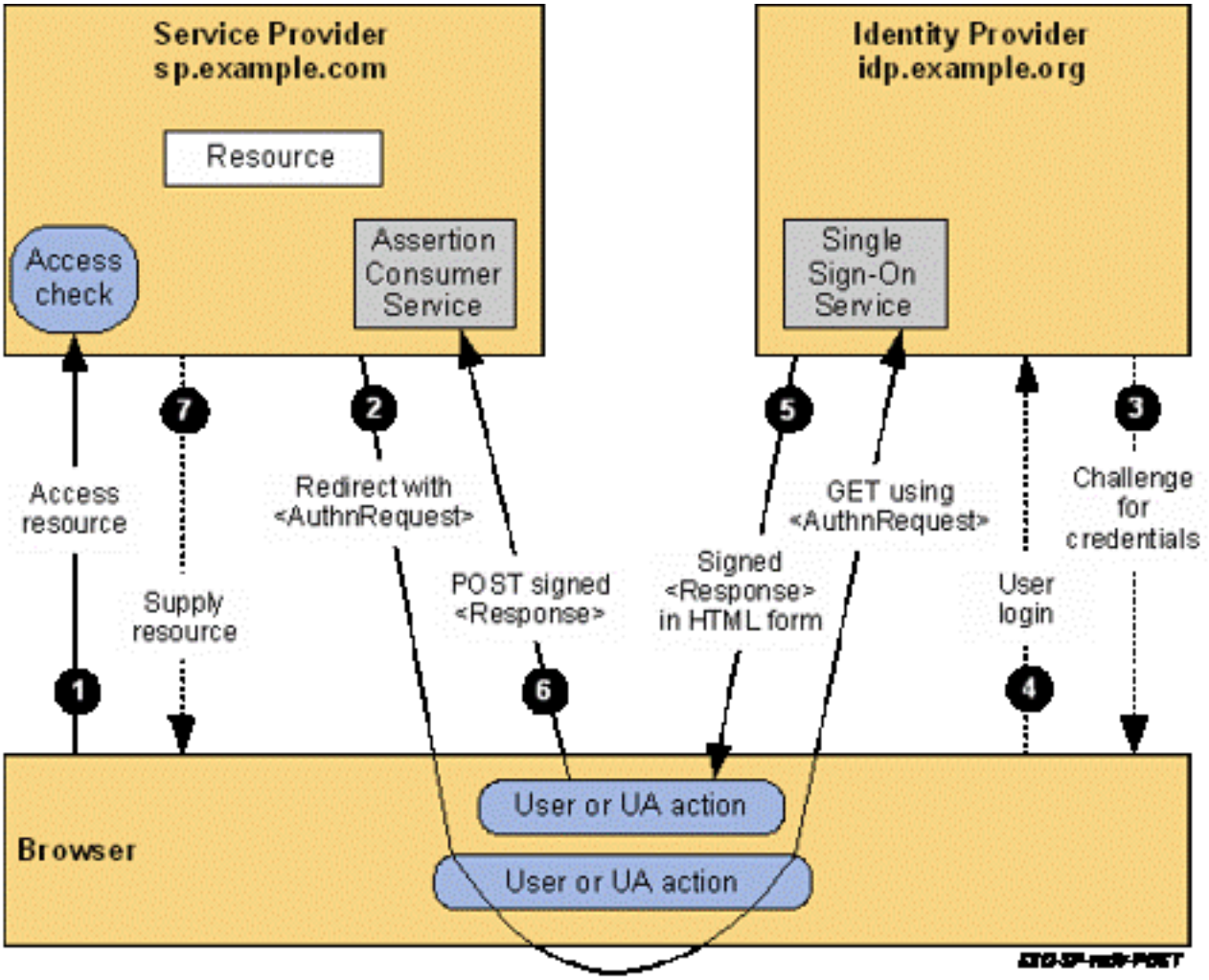
Les certificats jouent un rôle très important dans SSO et sont échangés entre le fournisseur de services et le fournisseur d'identité via des fichiers de métadonnées. Le fichier de métadonnées SP contient le certificat de signature et de chiffrement du fournisseur de services ainsi que d'autres informations importantes telles que les valeurs d'index de service Assertion Consume et les informations HTTP POST/REDIRECT. Le fichier de métadonnées IdP contient son ou ses certificats ainsi que d'autres informations sur les fonctionnalités IdP. Vous devez importer les métadonnées du fournisseur de services dans le fournisseur d'identité et importer les métadonnées du fournisseur d'identité dans le fournisseur de services pour créer un cercle de confiance. Le SP signe et chiffre essentiellement toute requête qu'il génère avec le certificat approuvé par le fournisseur d'identité, et le fournisseur d'identité signe et chiffre toute assertion (réponse) qu'il génère avec le ou les certificats approuvés par le fournisseur de services.

> **Note**: Si certaines informations sur le SP changent, telles que le nom d'hôte/nom de domaine complet (FQDN) ou le certificat de signature/cryptage (Tomcat ou ITLRecovery), le cercle de confiance peut être rompu. Vous devez télécharger un nouveau fichier de métadonnées à partir du SP et l'importer dans le fournisseur d'identités. Si certaines informations sur le fournisseur d'identité changent, vous devez télécharger un nouveau fichier de métadonnées à partir du fournisseur d'identité et réexécuter le test SSO afin de pouvoir mettre à jour les informations sur le fournisseur de services. Si vous n'êtes pas sûr que votre modification nécessite une mise à jour des métadonnées sur le périphérique opposé, il est préférable de mettre à jour le fichier. Il n'y a aucun inconvénient à une mise à jour des métadonnées de chaque côté et c'est une étape valide pour dépanner les problèmes SSO, surtout s'il y a eu un changement de configuration.

Configuration

Diagramme du réseau

Le flux d'une connexion SSO standard est illustré dans l'image :

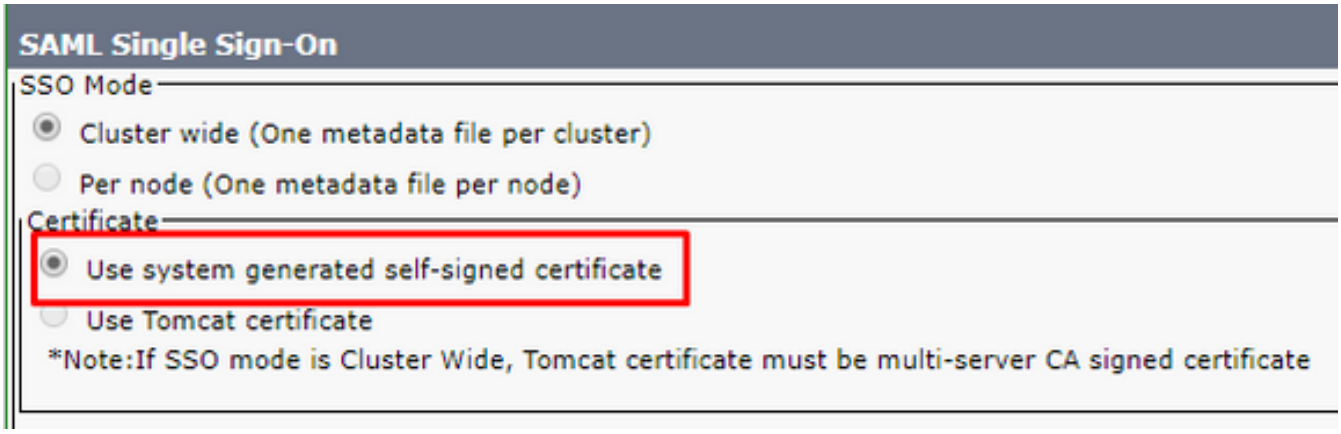


Note: Le processus de l'image n'est pas dans l'ordre de gauche à droite. N'oubliez pas que le fournisseur de services est CUCM et que le fournisseur d'identité est l'application tierce.

Configuration

Du point de vue de CUCM, il y a très peu à configurer en ce qui concerne SSO. Dans CUCM 11.5 et versions ultérieures, vous pouvez sélectionner l'authentification unique par noeud ou à l'échelle du cluster.

- Dans CUCM 11.5, l'authentification unique à l'échelle du cluster nécessite l'installation d'un certificat tomcat multiserveur sur tous les noeuds, car il n'y a qu'un seul fichier de métadonnées pour l'ensemble du cluster (et le certificat est stocké dans ce fichier, de sorte que vous avez besoin que chaque noeud ait le même certificat tomcat).
- Dans CUCM 12.0 et versions ultérieures, vous avez la possibilité d'**Utiliser** le **certificat autosigné généré par le système** pour l'authentification unique à l'échelle du cluster. Cette option utilise le certificat ITLRecovery plutôt que tomcat :



- L'authentification unique par noeud est la valeur par défaut antérieure à CUCM 11.5. Dans une configuration par noeud, chaque noeud dispose de son propre fichier de métadonnées qui doit être importé dans le fournisseur d'identité, car l'un de ces noeuds peut potentiellement rediriger un utilisateur pour authentification.
- Vous pouvez également activer SSO pour RTMT dans CUCM 11.5. Cette option est activée par défaut et se trouve dans **Cisco Unified CM Administration > Enterprise Parameters > Use SSO for RTMT**.

> **Note**: La note qui indique que **Si le mode SSO est Cluster Wide, le certificat Tomcat doit être un certificat CA signé multiserveur** est erroné sur 12.0 et 12.5 et un défaut a été ouvert pour le corriger (ID de bogue Cisco CSCvr49382).

Outre ces options, le reste de la configuration pour SSO se trouve sur le fournisseur d'identité. Les étapes de configuration peuvent varier considérablement en fonction du fournisseur d'identité que vous choisissez. Ces documents contiennent des étapes pour configurer certains des IdP les plus courants :

- Guide de configuration de Microsoft AD FS
- Guide de configuration Okta
- Guide de configuration PingFederate
- Guide de configuration Microsoft Azure

Dépannage

Données à collecter

Afin de dépanner un problème SSO, vous devez définir les traces SSO pour le débogage. Le niveau du journal SSO ne peut pas être défini sur debug via l'interface utilisateur graphique. Pour définir le niveau du journal SSO sur debug, exécutez cette commande dans l'interface de ligne de commande : **set samltrace level debug**

> **Note**: Cette commande ne s'applique pas à l'ensemble du cluster. Elle doit donc être exécutée sur chaque noeud pouvant être impliqué dans une tentative de connexion SSO.

Une fois que le niveau de journalisation a été défini sur debug, vous devez reproduire le problème et collecter ces données auprès de CUCM :

- Journaux Cisco SSO
- Journaux Cisco Tomcat

La plupart des problèmes SSO génèrent des exceptions ou des erreurs dans les journaux SSO, mais dans certains cas, les journaux Tomcat peuvent également être utiles.

Exemple d'analyse

Informations sur les périphériques du laboratoire TAC

CUCM (fournisseur de services) :

- Version : 12.5.1.14900-11
- Nom de domaine complet (FQDN) : 1cucm1251.sckiewer.lab

Windows Server 2016 (fournisseur d'identités) :

- Services de fédération Active Directory 3.0
- Nom de domaine complet (FQDN) : WinServer2016.sckiewer.lab

Examen du journal pour 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
1lbnQiIHhtbG5zOnhlbmM9Imh0dHA6Ly93d3cudzMub3JnLzIwMDEvMDQveG1sZW5jIyI+PHhlbmM6RW5jcnlwdGlvbk1ldG
hvZCBBbGdvcml0aG09Imh0dHA6Ly93d3cudzMub3JnLzIwMDEvMDQveG1sZW5jI2FlczI1Ni1jYmMiIC8+PEtleUluZm8geG
1sbnM9Imh0dHA6Ly93d3cudzMub3JnLzIwMDAvMDkveG1sZHNpZyMiPjxlOkVuY3J5cHRlZEtleSB4bWxuczplPSJodHRwOi
8vd3d3LnczLm9yZy8yMDAxLzA0L3htbGVuYyNiPjxlOkVuY3J5cHRpb25NZXRob2QgQWxnb3JpdGhtPSJodHRwOi8vd3Ln
czLm9yZy8yMDAxLzA0L3htbGVuYyNyc2Etb2FlcC1tZ2YxcCI+PERpZ2VzdE1ldGhvZCBBbGdvcml0aG09Imh0dHA6Ly93d3
cudzMub3JnLzIwMDAvMDkveG1sZHNpZyNzaGExIiAvPjwvZTpFbmNyeXB0aWdW0aG9kPjxLZXlJbmZvPjxkczpZ
F0YSB4bWxuczpkcz0iaHR0cDovL3d3dy53My5vcmcvMjAwMC8wOS94bWxkc2lnIyI+PGRzOlg1MDlJc3N1ZXJTZXJpYWw+PG
RzOlg1MDlJc3N1ZXJOYW1lPkw9UlRQLCBTPU5DLCBDTj1JVExSRUNPVkVSWV8xY3VjbTEyNTEuc2NraWV3ZXIubGFiLCBPVT
1UQUMsIE89Q2lzY28sIEM9VVM8L2RzOlg1MDlJc3N1ZXJOYW1lPjxkczpYNTA5U2VyaWFsTnVtYmVyPjEzNDkzNjAzNDA3Nz
A3NTkxMzA3MzMwMTI3MjY3OTM0NDY5MjA1MzwvZHM6WDUwOVNlcmlhbE51bWJlcj48L2RzOlg1MDlJc3N1ZXJTZXJpYWw+PC
9kczpYNTA5RGF0YT48L0tleUluZm8+PGU6Q2lwaGVyRGF0YT48ZTpDaXBoZXJWYWx1ZT5uRk9uN3RjNVFwZGV6SU1TTVMxc1
RBMW55aHNJTG5VQVRLakRkNUNMNkV0L3c3R2dVeEsrZkZsaDdhaGkzVFg1ZUcweEs4QkRXMXNORHM4dm94ZEYycTduL0xmck
FPTmg4ZzUzY1ZRZWN5TEtPaGlHZDNVZDNvazl5cHkwMmlZU1pYNkNMWGtGdGR5V0l6WUIzZDBwb0paeG5pdkRNUE8zMHEzbV
RwZmNQZVgzeTdGRU5UVS9DZ1Z3dkpTdllyNDRudnZmcmRHTm9DMTRhc2pqUHFvVXJ2MEN4TnUwNThCcGQwU25JSzdhSnRQaE
xya29OK1JNaWZVdzlzRWxIY0o1SVVkWE5wczhKVnNxaFBwZWpvYnZiSnBwRWM3QkdkT0ZZTW8yVWJmeTVSZ3M1UE4ya2lLTE
5YSVV0Qnh4emVxNi91VjlmbktYcFpqMy9KRWRRR3ZsOVE9PTwvZTpDaXBoZXJWYWx1ZT48L2U6Q2lwaGVyRGF0YT48L2U6RW
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
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: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+xcH2478M2Smm5mIVVINXnGW4N0U62hZz/aqIEm+3YAYTnvaytw9TFjld2rngkWzTIILAm6fslr9uZCVDHS37g0Ry2mUHYU0KHHXsbm/ouDS/F/LAm/w27X+5++U0o6g+NGE00QYwmo5hg+tNWmMxCnLtfENi8dGE+CSRv1oklLIx1QtK3mMI13WiebxOzp9ZP8IR5J1JxkkOWt9wSGBmZO7Gr7ZUmmEFpJ13qfKtcNZ9P8545rZ9UYHBcPH6H2uwYL0g8Awp5P74CAXHFwS1X2eg==</ds:SignatureValue><KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#"><ds:X509Data><ds:X509Certificate>MIIC8DCCAdigAwIBAgIQQ2RhydxzTY1GQQ88eF3LWjANBgkqhkiG9w0BAQsFADA0MTIwMAYDVQQDEylBREZTIFNpZ25pbmcgLSBXaW5TZXJ2ZXIyMDE2LnNja2lld2VyLmxhYjAeFw0xOTA0MTYxMjM0NDFaFw0yMDA0MTUxMjM0NDFaMDQxMjAwBgNVBAMTKUFERlMgU2lnbmluZyAtIFdpblNlcnZlcjIwMTYuc2NraWV3ZXIubGFiMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAsR20Nb3o8UqWeP8z17wkXJqIIYnqtbxiQXmdh4fJ4kNDno590dWFRjGTtcM+S44d6inis1lAfTWUgpsPWOCUgQWlA0o8Dyaq8UfiMIkt9ZrvMWc7krMCgILTC3m9eeCcypm9CdPZnuoL863yfRI+2TJr6j/nbUeIVL1KzJHcDgAVtcn/p/+0aHOC7GplC0yVI67FumWagVt9EaK+0SumclZYFyFTX641lfbpRbmcfAKrx0b10bfCkKDdCjgzXobuxlabzPp6IUb4NIsGIpm7fo7B23wHl/WIswu26XDp0IADbX25id9bRnR6GXRbfnYj1LBxCmpBq0VHsO1G7VwR4QIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQCPckMMbI7J/AQh62rFQbt2KFXJyyKCHhzQKai6hwMseM/eKScqOXG1VqPEjtbXx2XdqECZ8AJu64i6iaH1oMIcjxQtepZMHqMh/sKh1565oA23cFO5DttgXeEfyUBQe6R4lILi7m6IFapyPN3jL4+y4ggS/4VFVS02QPaQYZmTNnor2PPbOlMkq0mZO0D81MFk5ou1Np2zOGASq96/pa0Gi58BxyEZGCLbJlTe5v5dQnGHL3/f5BmIxduer7nUOvrEb+EdarxxwNHHRLB484j0W7GVQ/g6WVzvOGd1uAMdYfrW5Djw1W42Kv150eSh3RJg54Kr5EsoUidrz982Z+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"/></SubjectConfirmation></Subject><Conditions NotBefore="2021-04-30T13:01:03.891Z" NotOnOrAfter="2021-04-30T14:01:03.891Z"><AudienceRestriction><Audience>1cucm1251.sckiewer.lab</Audience></AudienceRestriction></Conditions><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

%%%%% 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::
```

Examen détaillé de la demande et de l'assertion SAML

Requête SAML

Analyse et informations sur la demande SAML :

```
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>
```

Affirmation

Analyse et informations sur la réponse SAML :

```
<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

Commandes CLI utiles

- utils sso disable : permet de désactiver SSO si celui-ci ne fonctionne pas
- utils sso status : indique l'état actuel de SSO sur le noeud
- utils so recovery-url enable - Permet de désactiver l'URL de récupération

- utils so recovery-url disable : permet d'activer l'URL de récupération
- show samltrace level - Affiche le niveau de journal actuel pour les journaux SSO
- set samltrace level : permet de définir le niveau de journalisation des journaux SSO. Vous devez définir cette option sur DEBUG pour que nous puissions résoudre efficacement les problèmes.

Passer de AssertionConsumerServiceURL à AssertionConsumerServiceIndex

Lorsque l'authentification unique à l'échelle du cluster a été ajoutée dans CUCM 11.5, CUCM n'écrit plus l'URL AssertionConsumerService (ACS) dans la requête SAML. À la place, CUCM écrit l'AssertionConsumerServiceIndex. Voir ces extraits d'une requête SAML :

CUCM avant 11.5.1 :

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

CUCM 11.5.1 et versions ultérieures :

```
AssertionConsumerServiceIndex="0"
```

Dans les versions 11.5 et ultérieures, CUCM s'attend à ce que l'IdP utilise le numéro d'index ACS de la demande afin de rechercher l'URL ACS à partir du fichier de métadonnées qui a été téléchargé pendant le processus de configuration. Cet extrait de métadonnées CUCM affiche l'URL POST de l'éditeur associée à l'index 0 :

```
<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"/>
```

Il n'existe aucune solution de contournement pour modifier ce comportement et le fournisseur d'identité doit utiliser les valeurs d'index ACS plutôt que l'URL ACS. Vous trouverez plus d'informations ici, ID de bogue Cisco CSCvc56596.

Problèmes courants

Impossible d'accéder à l'administration du SE ou à la reprise après sinistre

Dans CUCM 12.x, les applications Web Cisco Unified OS Administration et Disaster Recovery System utilisent SSO. Si les tentatives de connexion à ces applications échouent avec une erreur 403 après l'activation de SSO, cela est probablement dû au fait que la plate-forme CUCM est incapable de trouver l'ID utilisateur. Cela se produit parce que ces applications ne référencent pas la table des utilisateurs finaux utilisée par CM Administration, Serviceability et Reporting. De ce fait, l'ID utilisateur que le fournisseur d'identité a authentifié n'existe pas du côté de la plate-forme CUCM. CUCM retourne donc un 403 Forbidden. Ce document explique comment ajouter les utilisateurs appropriés dans le système afin que les applications de la plate-forme utilisent SSO avec succès.

Échec NTP

SSO est sensible au temps en raison du fait que le fournisseur d'identité associe un « délai de

validité » aux assertions. Afin de vérifier si l'heure est le problème dans votre cas, vous pouvez rechercher cette section dans les journaux SSO :

```
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
```

Si vous trouvez **Time Valid?:false** dans vos journaux SSO, examinez la section Conditions de l'assertion pour identifier le délai dans lequel l'assertion doit être considérée comme valide :

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

Vous pouvez voir dans l'extrait d'exemple que cette assertion n'est valide que de 13:01:03:8917 à 14:01:03:8917 le 30/04/2021. Dans un scénario d'échec, référez-vous à l'heure à laquelle CUCM a reçu cette assertion et vérifiez qu'elle se trouve dans la période de validité de l'assertion. Si le temps que CUCM a traité la déclaration est en dehors de la période de validité, c'est la cause de votre problème. Assurez-vous que CUCM et le fournisseur d'identité se synchronisent tous deux sur le même serveur NTP car l'authentification unique est très sensible au temps.

Instruction d'attribut non valide

Référez-vous à l'analyse de l'assertion ici et consultez la note sur l'instruction d'attribut. Les produits Cisco Unified Communications nécessitent une déclaration d'attribut fournie par le fournisseur d'identité, mais parfois ce dernier n'en envoie pas. Pour référence, il s'agit d'un AttributeStatement valide :

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

Si vous voyez une assertion du fournisseur d'identité, mais que l'instruction d'attribut est omise, vous devez travailler avec le fournisseur de votre logiciel de fournisseur d'identité pour apporter les modifications nécessaires afin qu'il fournisse cette instruction. Le correctif diffère selon le fournisseur d'identité et dans certains scénarios, il est possible d'envoyer plus d'informations dans cette instruction que dans l'extrait de code. Tant qu'un nom d'attribut est défini sur uid et qu'un AttributeValue correspond à un utilisateur disposant des privilèges appropriés dans la base de données CUCM, la connexion réussit.

Deux certificats de signature - AD FS

Ce problème est spécifique à Microsoft AD FS. Lorsque le certificat de signature sur AD FS est sur le point d'expirer, Windows Server génère automatiquement un nouveau certificat, mais laisse l'ancien certificat en place jusqu'à son expiration. Dans ce cas, les métadonnées AD FS contiennent deux certificats de signature. Le message d'erreur que vous pouvez voir lorsque vous tentez d'exécuter le test SSO pendant cette période est, **Error while processing SAML response**.

Remarque : Une erreur lors du traitement de la réponse SAML peut également être présentée pour d'autres problèmes. Ne supposez donc pas qu'il s'agit de votre problème si vous voyez cette erreur. Assurez-vous de vérifier les journaux SSO.

Si vous voyez cette erreur, consultez les journaux SSO et recherchez ceci :

```
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.
```

Cette erreur indique que les métadonnées IdP importées dans CUCM contiennent un certificat de signature qui ne correspond pas à ce que l'IdP a utilisé dans cet échange SAML. Cette erreur se produit généralement parce qu'AD FS a deux certificats de signature. Lorsque le certificat d'origine est sur le point d'expirer, AD FS génère automatiquement un nouveau certificat. Vous devez télécharger un nouveau fichier de métadonnées à partir d'AD FS, vérifier qu'il ne possède qu'un seul certificat de signature et de chiffrement et l'importer dans CUCM. D'autres IDp ont également des certificats de signature qui doivent être mis à jour afin qu'il soit possible que quelqu'un l'ait mis à jour manuellement mais n'ait tout simplement pas importé le nouveau fichier de métadonnées qui contient le nouveau certificat dans CUCM.

Si vous rencontrez les erreurs mentionnées :

- Si vous utilisez AD FS, référez-vous à l'ID de bogue Cisco CSCuj66703
- Si vous n'utilisez PAS AD FS, collectez un nouveau fichier de métadonnées à partir de l'IdP et importez-le dans CUCM

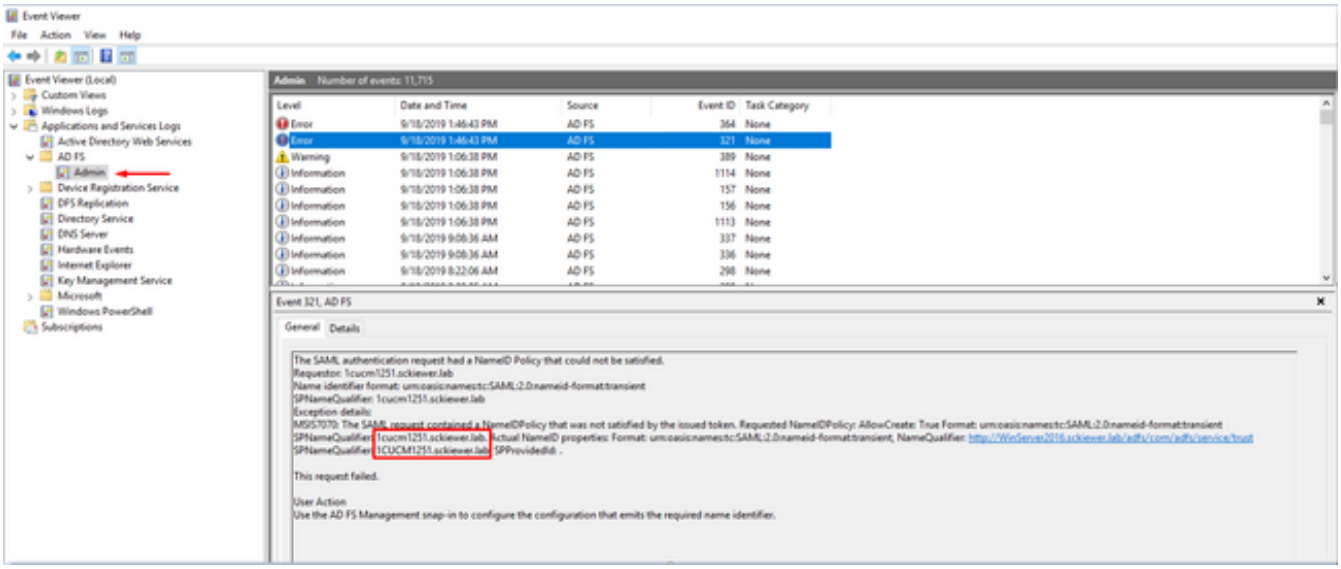
Code d'état non valide dans la réponse

Il s'agit d'une erreur courante dans les déploiements avec 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.
```

Dans presque tous les cas, il s'agit d'un problème avec la règle de revendication du côté AD FS. Je vous recommande de coller d'abord la règle dans le bloc-notes, d'ajouter vos ID d'entité, puis de coller la règle du bloc-notes dans AD FS. Dans certains cas, un copier/coller directement à partir de votre e-mail ou de votre navigateur peut omettre une partie de la ponctuation et provoquer une erreur de syntaxe.

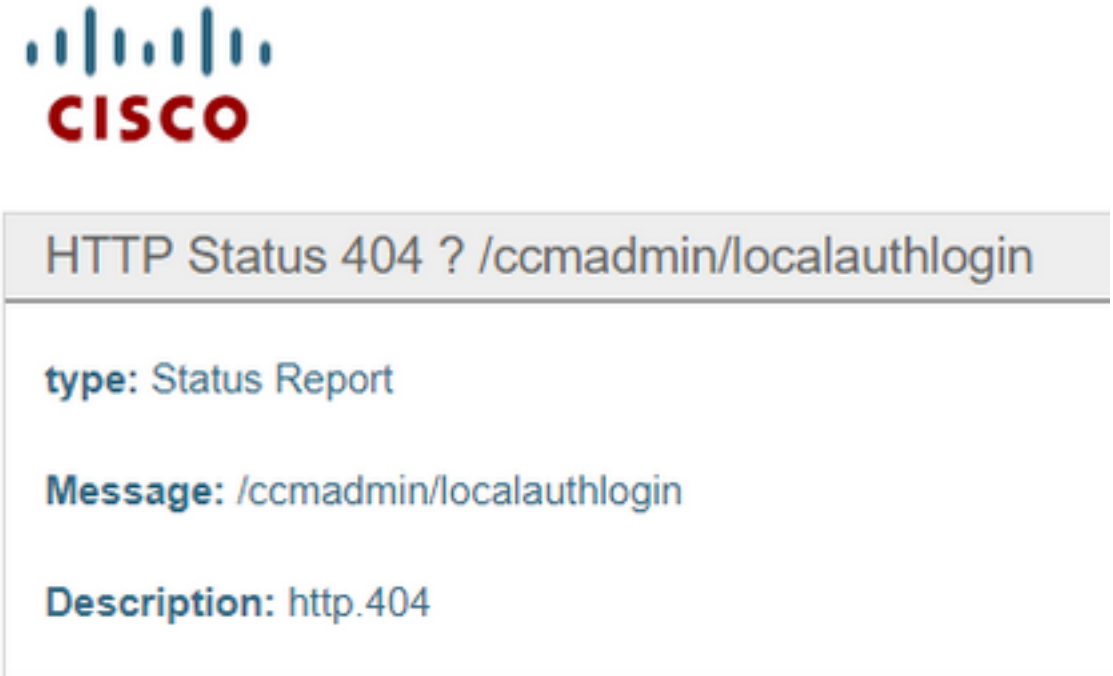
La règle de revendication présente un autre problème courant : la casse des noms de domaine complets (FQDN) du fournisseur d'identité ou du fournisseur de services ne correspond pas à l'ID d'entité dans les fichiers de métadonnées. Vous devez vérifier les journaux de l'Observateur d'événements sur le serveur Windows pour déterminer s'il s'agit de votre problème.



Vous pouvez voir dans l'image que l'ID de nom demandé est 1cucm1251.sckiewer.lab tandis que l'ID de nom réel est 1CUCM1251.sckiewer.lab. L'ID de nom demandé doit correspondre à l'ID d'entité dans le fichier de métadonnées SP tandis que l'ID de nom réel est défini dans la règle de revendication. Pour résoudre ce problème, je dois mettre à jour la règle de revendication avec un nom de domaine complet en minuscules pour le SP.

Incompatibilité d'état SSO entre CLI et GUI

Dans certains cas, **utils so status** et l'interface graphique utilisateur peuvent afficher des informations différentes sur l'activation ou la désactivation de l'authentification unique. La façon la plus simple de résoudre ce problème est de désactiver et de réactiver SSO. Il y a un certain nombre de fichiers et de références qui sont mis à jour par le processus d'activation, il n'est donc pas possible d'essayer de mettre à jour manuellement tous ces fichiers. Dans la plupart des cas, vous pouvez vous connecter à l'interface utilisateur graphique et désactiver et réactiver sans problème, cependant, il est possible de voir cette erreur lorsque vous essayez d'accéder à l'éditeur via URL de récupération ou le lien principal :



Vous pouvez vérifier l'interface graphique pour voir si l'URL de récupération est une option et vous pouvez également vérifier le résultat **utils so status** de l'interface de ligne de commande :

```
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
```

Vous devez ensuite vérifier la table des noeuds de processus. Dans cet exemple, vous pouvez voir que SSO est désactivé dans la base de données (voir la valeur tkssomode pour 1cucm1251.sckiewer.lab à l'extrême droite) :

```
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
```

Pour résoudre ce problème, vous devez redéfinir le champ tkssomode de la table des noeuds de processus sur 2 afin de pouvoir vous connecter via l'URL de récupération :

```
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
```

Àce stade, testez l'URL de récupération et continuez avec une **Désactiver > Réactiver SSO** qui déclenche CUCM pour mettre à jour toutes les références dans le système.

Informations connexes

- Guide de déploiement de SAML SSO pour les applications Cisco Unified Communications, version 12.5(1)
- Présentation technique du langage SAML (Security Assertion Markup Language) version 2.0
- Support et documentation techniques - Cisco Systems

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.