

Configurazione e risoluzione dei problemi di SSO su Cisco Unified Communications Manager (CUCM)

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Circolo di fiducia](#)

[Configurazione](#)

[Esempio di rete](#)

[Configurazione](#)

[Risoluzione dei problemi](#)

[Dati da raccogliere](#)

[Analisi di esempio](#)

[Informazioni sul dispositivo da TAC lab](#)

[Esame del log per CUCM](#)

[Descrizione dettagliata della richiesta e dell'asserzione SAML](#)

[Richiesta SAML](#)

[Asserzione](#)

[Comandi CLI utili](#)

[Modifica da AssertionConsumerServiceURL a AssertionConsumerServiceIndex](#)

[Problemi comuni](#)

[Impossibile accedere all'amministrazione del sistema operativo o al ripristino di emergenza](#)

[Errore NTP](#)

[Istruzione di attributo non valida](#)

[Due certificati di firma - ADFS](#)

[Codice di stato non valido nella risposta](#)

[Stato SSO non corrispondente tra CLI e GUI](#)

[Informazioni correlate](#)

Introduzione

Questo documento descrive la funzione SSO in CUCM, la configurazione, i suggerimenti per la risoluzione dei problemi, l'analisi di log di esempio e le risorse per ulteriori informazioni.

Prerequisiti

Requisiti

Cisco consiglia di conoscere alcuni termini Single Sign-On (SSO):

- SAML (Security Assertion Markup Language): uno standard aperto per lo scambio di dati di autenticazione e autorizzazione tra le parti
- Service Provider (SP) - L'SP è l'entità che ospita il servizio. In questo documento, Cisco Unified Communications Manager (CUCM) è il provider di servizi
- Provider di identità (IdP) - L'IdP è l'entità che autentica le credenziali client. L'autenticazione è completamente trasparente per l'SP in modo che le credenziali possano essere una smart card, un nome utente/password e così via. Dopo aver autenticato le credenziali del client, IdP genera un'asserzione, la invia al client e reindirizza il client all'SP
- Asserzioni: informazioni sensibili al tempo generate dall'IdP dopo l'autenticazione di un utente. Lo scopo dell'asserzione è quello di fornire informazioni sull'utente autenticato all'SP
- Binding: definisce il metodo di trasporto utilizzato per il recapito dei messaggi del protocollo SAML tra le entità. I prodotti Cisco Unified Communications utilizzano il protocollo HTTP
- Profili: vincoli predefiniti e combinazioni di contenuti di messaggi SAML (asserzioni, protocolli, associazioni) che consentono di ottenere uno specifico caso di utilizzo aziendale. Questo corso è incentrato sul profilo Single Sign-On del browser Web in quanto è il metodo utilizzato da CUCM
- Metadati: set di informazioni di configurazione scambiate tra le parti. Contiene informazioni quali associazioni SAML supportate, ruoli operativi quali IdP o SP, attributi di identificatore supportati, informazioni sugli identificatori e informazioni sui certificati utilizzate per firmare e crittografare la richiesta o la risposta.

Componenti usati

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

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Lo scopo dell'SSO è quello di consentire a utenti e amministratori di accedere a più applicazioni di collaborazione Cisco senza richiedere autenticazioni separate per ognuna di esse. L'attivazione dell'SSO comporta diversi vantaggi:


- Migliora la produttività perché gli utenti non devono immettere nuovamente le credenziali per la stessa identità su prodotti diversi.
- Trasferisce l'autenticazione dal sistema che ospita le applicazioni a un sistema di terze parti. Si crea un cerchio di fiducia tra un provider di identità e un provider di servizi che consente

all'provider di identità di autenticare gli utenti per conto dell'SP.

- Fornisce la crittografia per proteggere le informazioni di autenticazione passate tra l'IdP, il provider di servizi e l'utente. SSO nasconde inoltre i messaggi di autenticazione passati tra l'IdP e il provider di servizi da qualsiasi parte esterna.
- Consente di ridurre i costi grazie al minor numero di chiamate all'help desk per la reimpostazione della password.

Circolo di fiducia

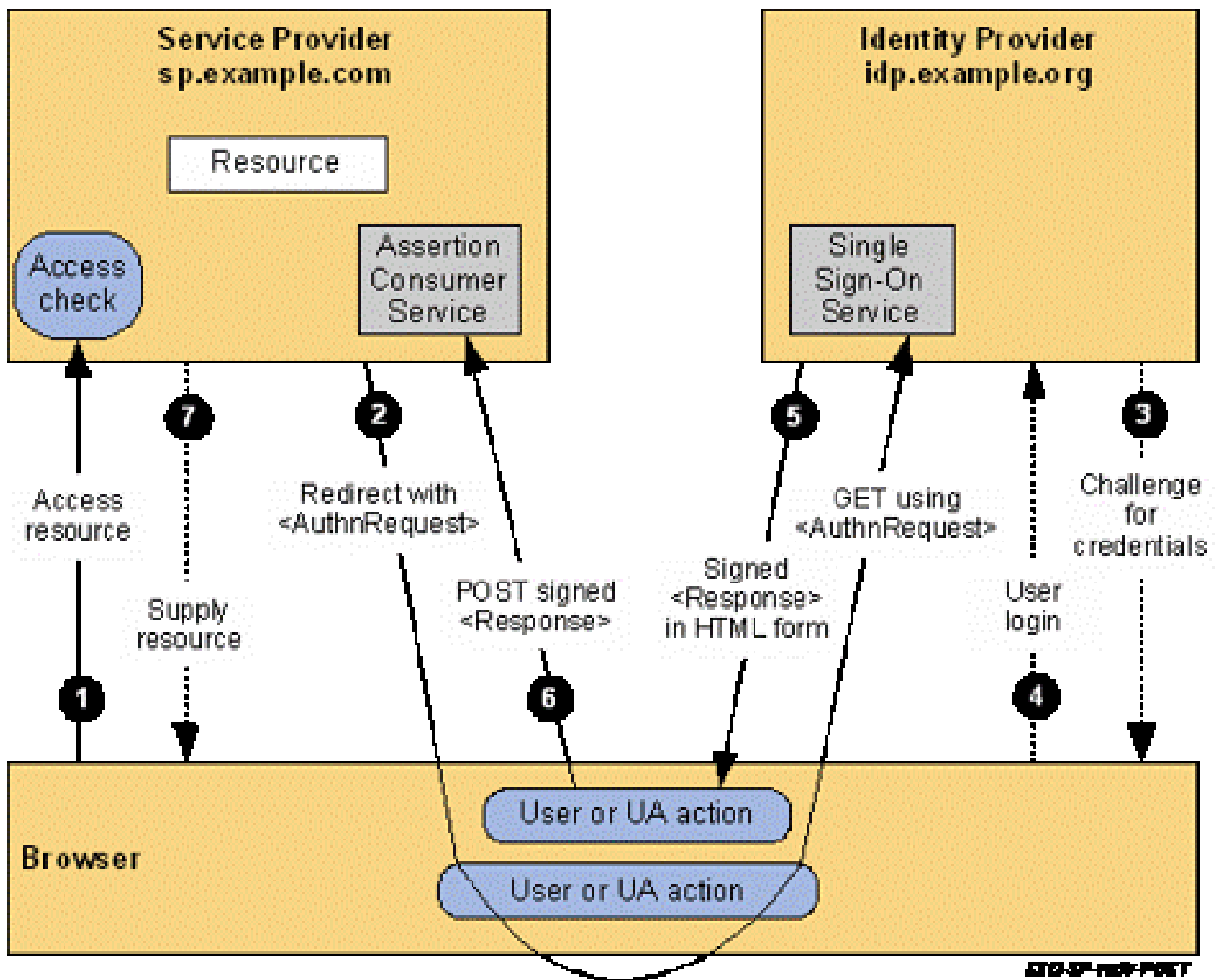
I certificati svolgono un ruolo molto importante nell'SSO e vengono scambiati tra l'SP e l'IdP tramite file di metadati. Il file di metadati SP contiene il certificato di firma e crittografia del provider di servizi insieme ad altre importanti informazioni, quali i valori Assertion Use Service Index e le informazioni HTTP POST/REDIRECT. Il file di metadati IdP contiene i relativi certificati insieme ad altre informazioni sulle funzionalità IdP. È necessario importare i metadati SP nell'IdP e importare i metadati IdP nell'SP per creare un circolo di fiducia. In pratica, l'SP firma e crittografa qualsiasi richiesta generata con il certificato considerato attendibile dall'IdP, mentre l'IdP firma e crittografa qualsiasi asserzione (risposta) generata con certificati considerati attendibili dall'SP.


 Nota: se vengono modificate determinate informazioni sull'SP, ad esempio il nome host/nome di dominio completo (FQDN) o il certificato di firma/crittografia (Tomcat o ITLRecovery), è possibile interrompere il circolo di fiducia. Scaricare un nuovo file di metadati dall'SP e importarlo nell'IdP. Se determinate informazioni sull'IdP vengono modificate, scaricare un nuovo file di metadati dall'IdP ed eseguire nuovamente il test SSO in modo da poter aggiornare le informazioni sull'SP. Se non si è certi che la modifica richieda un aggiornamento dei metadati sul dispositivo opposto, è consigliabile aggiornare il file. Non ci sono vantaggi per un aggiornamento dei metadati da entrambi i lati e questo è un passo valido per risolvere i problemi di SSO, soprattutto se c'è stata una modifica alla configurazione.

Configurazione

Esempio di rete

Il flusso per un accesso SSO standard è mostrato nell'immagine:



 Nota: il processo nell'immagine non è in ordine da sinistra a destra. Tenere presente che l'SP è CUCM e l'IdP è l'applicazione di terze parti.

Configurazione

Dal punto di vista di CUCM, c'è molto poco da configurare per quanto riguarda l'SSO. In CUCM 11.5 e versioni successive è possibile selezionare SSO cluster o per nodo.

- In CUCM 11.5, l'SSO a livello di cluster richiede l'installazione di un certificato tomcat multiserver su tutti i nodi poiché esiste un solo file di metadati per l'intero cluster (e il certificato è archiviato in tale file, quindi ogni nodo deve avere lo stesso certificato tomcat).
- In CUCM 12.0 e versioni successive è possibile utilizzare il certificato autofirmato generato dal sistema per l'SSO a livello di cluster. Questa opzione utilizza il certificato ITLRecovery anziché tomcat:

SAML Single Sign-On

SSO Mode


- Cluster wide (One metadata file per cluster)
- Per node (One metadata file per node)

Certificate

- Use system generated self-signed certificate
- Use Tomcat certificate

*Note: If SSO mode is Cluster Wide, Tomcat certificate must be multi-server CA signed certificate

- L'SSO per nodo è l'impostazione predefinita precedente a CUCM 11.5. In una configurazione per nodo, ogni nodo dispone di un proprio file di metadati che deve essere importato nell'IdP poiché uno qualsiasi di questi nodi può potenzialmente reindirizzare un utente per l'autenticazione.
- È inoltre possibile abilitare SSO per RTMT in CUCM 11.5. Questa opzione è abilitata per impostazione predefinita e si trova in Cisco Unified CM Administration > Enterprise Parameters > Use SSO for RTMT (Amministrazione Cisco Unified CM > Parametri aziendali > Usa SSO per RTMT).

 Nota: la nota che indica che se la modalità SSO è estesa a tutto il cluster, il certificato Tomcat deve essere firmato da una CA con più server è errato nelle versioni 12.0 e 12.5 ed è stato aperto un difetto per correggerlo (ID bug Cisco [CSCvr49382](#)).


A parte queste opzioni, il resto della configurazione per SSO è sull'IdP. I passaggi di configurazione possono variare notevolmente in base all'IdP scelto. In questi documenti viene descritto come configurare alcuni degli IdP più comuni:

- [Guida alla configurazione di Microsoft AD FS](#)
- [Guida Alla Configurazione Di Okta](#)
- [Guida alla configurazione di PingFederate](#)
- [Guida alla configurazione di Microsoft Azure](#)

Risoluzione dei problemi

Dati da raccogliere

Per risolvere un problema relativo all'SSO, impostare le tracce dell'SSO su debug. Impossibile impostare il livello di log SSO per il debug tramite GUI. Per impostare il livello di log SSO su debug, eseguire questo comando nella CLI: `set samltrace level debug`

 Nota: questo comando non è a livello di cluster, pertanto deve essere eseguito su ogni nodo che potrebbe essere coinvolto in un tentativo di accesso SSO.

Dopo aver impostato il livello di log per il debug, riprodurre il problema e raccogliere i seguenti dati

da CUCM:

- Log SSO Cisco
- Log di Cisco Tomcat

La maggior parte dei problemi di SSO genera eccezioni o errori nei log SSO, ma in alcune circostanze possono essere utili anche i log Tomcat.

Analisi di esempio

Informazioni sul dispositivo da TAC lab

CUCM (provider di servizi):

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

Windows Server 2016 (provider di identità):

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

Esame del log per 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 :/showHom

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

%%%% You can see the SP and IdP EntityIDs here

2021-04-30 09:00:53,194 DEBUG [http-bio-443-exec-83] fappend.SamlLogger - SPSSOFederate: spEntityID is

2021-04-30 09:00:53,194 DEBUG [http-bio-443-exec-83] fappend.SamlLogger - SPSSOFederate: idpEntityID :

%%%% The client is redirected to the SSO URL listed here

2021-04-30 09:00:53,196 DEBUG [http-bio-443-exec-83] fappend.SamlLogger - SPSSOFederate: SingleSignOnSe

%%%% CUCM prints the AssertionConsumerService URL and you can see that CUCM uses an HTTP-POST

2021-04-30 09:00:53,196 DEBUG [http-bio-443-exec-83] fappend.SamlLogger - SPSSOFederate: AssertionConsum

2021-04-30 09:00:53,196 DEBUG [http-bio-443-exec-83] fappend.SamlLogger - SPSSOFederate: AssertionConsum

2021-04-30 09:00:53,196 DEBUG [http-bio-443-exec-83] fappend.SamlLogger - SPSSOFederate: AssertionConsum

%%%% Here CUCM prints the AuthnRequest to the client. The client is redirected to the IdP with a 302 a

2021-04-30 09:00:53,199 DEBUG [http-bio-443-exec-83] fappend.SamlLogger - SPSSOFederate: AuthnRequest:<

ID="s29fd87c888ef6a4bc8c48d7e7087a8aeb997dd76f" Version="2.0" IssueInstant="2021-04-30T13:00:53Z" Desti

<saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">1cucm1251.sckiewer.lab</saml:Issuer>

<samlp:NameIDPolicy xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" Format="urn:oasis:names:tc:SAML:

</samlp:AuthnRequest>

%%%% You can see that CUCM has received an encoded SAML response that is base64 encoded

2021-04-30 09:01:03,986 DEBUG [http-bio-8443-exec-85] authentication.SAMLAuthenticator - SAML Response

%%%% Here is the encrypted SAML response from the client. You can see that the InResponseTo value match

2021-04-30 09:01:04,005 DEBUG [http-bio-8443-exec-85] fappend.SamlLogger - SPACSUtils.getResponse: got

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

%%%% Here you can see that the IdP uses a supported binding type

```
2021-04-30 09:01:04,010 DEBUG [http-bio-8443-exec-85] fappend.SamlLogger - SAML2Utils.verifyResponse:bi
```

%%%% The decrypted assertion is printed here. You see that a lot of important information covered late

```
2021-04-30 09:01:04,090 DEBUG [http-bio-8443-exec-85] authentication.SAMLAuthenticator - <Assertion xml
```

%%%% CUCM looks at its current time and makes sure that it is within the validity timeframe of the ass

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

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

```
2021-04-30 09:01:04,090 DEBUG [http-bio-8443-exec-85] authentication.SAMLAuthenticator - Attributes: {u
```

%%%% CUCM prints the username here

```
2021-04-30 09:01:04,090 DEBUG [http-bio-8443-exec-85] authentication.SAMLAuthenticator - userid is ::ad
```

```
2021-04-30 09:01:04,090 DEBUG [http-bio-8443-exec-85] authentication.SAMLAuthenticator - Realy state is
```

```
2021-04-30 09:01:04,091 DEBUG [http-bio-8443-exec-85] authentication.SAMLAuthenticator - http request c
```

%%%% The client is redirected to the resource it initially tried to access

```
2021-04-30 09:01:04,283 INFO [http-bio-8443-exec-85] servlet.RelayToOriginalAppServlet - relayUrl ::/cc
```

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

Descrizione dettagliata della richiesta e dell'asserzione SAML

Richiesta SAML

Analisi e informazioni sulla richiesta 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 c

%%%% This log snippet was taken from CUCM 12.5, so you use the AssertionConsumerServiceIndex rather th

```
ID="s29fd87c888ef6a4bc8c48d7e7087a8aeb997dd76f" Version="2.0" IssueInstant="2021-04-30T13:00:53Z" Desti
```

```
<saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">1cucm1251.sckiewer.lab</saml:Issuer>
```

%%%% The NameID Format must be transient.

%%%% The SP Name Qualifier allows us to see which node generated the request.

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

```
</samlp:AuthnRequest>
```

Asserzione

Analisi e informazioni sulla risposta SAML:

```
<#root>
```

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

%% You can see that the issuer of the assertion was my Windows server

```
<Issuer>http://WinServer2016.sckiewer.lab/adfs/services/trust</Issuer>
<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<ds:SignedInfo>
<ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
<ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256" />
<ds:Reference URI="#_23d2b89f-7e75-4dc8-b154-def8767a391c">
<ds:Transforms>
<ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
<ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
</ds:Transforms>
<ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmldsig#sha256" />
<ds:DigestValue>aYn1NK8NiHWHshYMggpeDsta2GyUKQI5MmRmx+gI374=</ds:DigestValue>
</ds:Reference>
</ds:SignedInfo>
<ds:SignatureValue>rvkc6QWoTCLD1y8/MoRCzGcu0FJR6PSu5BTQt3qp5ua7J/AQbbzWn7gWK6TzI+xcH2478M2Smm5mIVVINXnG
<KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
<ds:X509Data>
<ds:X509Certificate>MIIC8DCCAdigAwIBAgIQQ2RhydxyzTY1GQQ88eF3LWjANBgkqhkiG9w0BAQsFADAOMTIwMAYDVQQDEy1BREZ
</ds:X509Data>
</KeyInfo>
</ds:Signature>
<Subject>
```

%% The NameID Format is transient which is what CUCM expects

```
<NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient" NameQualifier="http://WinServer201
<SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
```

%% You have an InResponseTo value that matches our SAML request, so you can correlate a given assert

```
<SubjectConfirmationData InResponseTo="s29fd87c888ef6a4bc8c48d7e7087a8aeb997dd76f" NotOnOrAfter="2021-0
</SubjectConfirmation>
</Subject>
```

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

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

%% AttributeStatement is a required section that provides the ID of the user (admin in this case) an

```
<AttributeStatement>
<Attribute Name="uid">
<AttributeValue>admin</AttributeValue>
</Attribute>
</AttributeStatement>
<AuthnStatement AuthnInstant="2021-04-30T13:01:03.844Z" SessionIndex="_23d2b89f-7e75-4dc8-b154-def8767a
<AuthnContext>
<AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes>PasswordProtectedTransport</AuthnContextCl
</AuthnContext>
</AuthnStatement>
</Assertion> XML Representation
```


Comandi CLI utili

- `utilizza sso disable` - Consente di disabilitare SSO se non è funzionante
- `utils sso status`: visualizza lo stato corrente di SSO sul nodo.
- `utilizza sso recovery-url enable`: consente di disabilitare l'URL di ripristino
- `utils sso recovery-url disable` - Consente di abilitare l'URL di ripristino
- `show samltrace level`: visualizza il livello di log corrente per i log SSO
- `set samltrace level` - Consente di impostare il livello di log per i log SSO. Questa opzione deve essere impostata su `DEBUG` per consentire una risoluzione efficace dei problemi.

Modifica da `AssertionConsumerServiceURL` a `AssertionConsumerServiceIndex`

Quando l'SSO a livello di cluster è stato aggiunto in CUCM 11.5, CUCM non scrive più l'URL `AssertionConsumerService` (ACS) nella richiesta SAML. Viene invece scritto `AssertionConsumerServiceIndex`. Vedere questi snippet da una richiesta SAML:

CUCM precedente alla 11.5.1:

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

CUCM 11.5.1 e versioni successive:

```
AssertionConsumerServiceIndex="0"
```

Nella versione 11.5 e successive, CUCM si aspetta che l'IdP utilizzi il numero di indice ACS della richiesta per cercare l'URL ACS dal file di metadati caricato durante il processo di configurazione. In questo frammento di metadati CUCM viene visualizzato l'URL POST (del server di pubblicazione) associato all'indice 0:

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

Non sono disponibili soluzioni alternative per modificare questo comportamento e l'IdP deve utilizzare i valori di indice ACS anziché l'URL ACS. Per ulteriori informazioni, consultare l'ID bug Cisco [CSCvc56596](#).

Problemi comuni

Impossibile accedere all'amministrazione del sistema operativo o al ripristino di

emergenza

In CUCM 12.x, le applicazioni Web Cisco Unified OS Administration and Disaster Recovery System utilizzano l'SSO. Se i tentativi di accesso a queste applicazioni falliscono con un errore 403 dopo l'abilitazione dell'SSO, è probabile che la piattaforma CUCM non sia in grado di trovare l'ID utente. Ciò si verifica perché queste applicazioni non fanno riferimento alla tabella degli utenti finali utilizzata da Amministrazione CM, Serviceability e Reporting. Per questo motivo, l'ID utente autenticato dall'IdP non esiste sul lato piattaforma CUCM, pertanto CUCM restituisce un 403 Vietato. [In questo documento](#) viene descritto come aggiungere gli utenti appropriati al sistema in modo che le applicazioni della piattaforma utilizzino correttamente l'SSO.

Errore NTP

L'SSO è sensibile al tempo in quanto IdP associa un 'intervallo di tempo di validità' alle asserzioni. Per verificare se il problema riguarda l'ora, è possibile cercare questa sezione nei log SSO:

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

Se si trova Time Valid?:false nei log SSO, esaminare la sezione Condizioni dell'asserzione per identificare l'intervallo di tempo in cui l'asserzione deve essere considerata valida:

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

Nello snippet di esempio è possibile vedere che questa asserzione è valida solo dalle 13:01:03:8917 alle 14:01:03:8917 del 30/04/2021. In uno scenario di errore, fare riferimento all'ora in cui CUCM ha ricevuto questa asserzione e verificare che sia compresa nel periodo di validità dall'asserzione. Se l'ora in cui il CUCM ha elaborato l'asserzione non è compresa nel periodo di validità, questa è la causa del problema. Verificare che CUCM e IdP siano sincronizzati allo stesso server NTP poiché l'SSO richiede molto tempo.

Istruzione di attributo non valida

Fare riferimento all'analisi dell'asserzione [qui](#) e vedere la nota sull'istruzione attribute. I prodotti Cisco Unified Communications richiedono che l'IdP fornisca un'istruzione di attributo, ma a volte l'IdP non la invia. Per riferimento, si tratta di un AttributeStatement valido:


```
<AttributeStatement>
```

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

Se viene visualizzata un'asserzione dell'IdP, ma l'istruzione dell'attributo viene omessa, collaborare con il fornitore del software dell'IdP per apportare le modifiche necessarie in modo che fornisca tale istruzione. La correzione varia in base all'IdP e in alcuni scenari è possibile inviare in questa istruzione più informazioni di quelle visualizzate nello snippet. L'accesso viene eseguito correttamente se il nome dell'attributo è impostato su uid e se AttributeValue corrisponde a un utente con i privilegi corretti nel database CUCM.

Due certificati di firma - ADFS

Questo problema è specifico di Microsoft AD FS. Quando il certificato di firma in ADFS è prossimo alla scadenza, in Windows Server viene generato automaticamente un nuovo certificato, ma il vecchio certificato rimane in vigore fino alla scadenza. In questo caso, i metadati ADFS contengono due certificati di firma. Il messaggio di errore che è possibile visualizzare quando si tenta di eseguire il test SSO durante questo intervallo di tempo è, Errore durante l'elaborazione della risposta SAML.

 Nota: errore durante l'elaborazione della risposta SAML può essere presentato anche per altri problemi, quindi non presumere che questo sia il problema che si verifica se viene visualizzato questo errore. Accertarsi di controllare i registri SSO da verificare.

Se viene visualizzato questo errore, esaminare i log SSO e cercare quanto segue:

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

Questo errore indica che i metadati IdP importati in CUCM contengono un certificato di firma che non corrisponde a quello utilizzato in questo scambio SAML. Questo errore si verifica in genere perché ADFS dispone di due certificati di firma. Quando il certificato originale è prossimo alla scadenza, ADFS genera automaticamente un nuovo certificato. È necessario scaricare un nuovo file di metadati da ADFS, verificare che disponga di un solo certificato di firma e crittografia e importarlo in CUCM. Anche altri IdP dispongono di certificati di firma che devono essere aggiornati in modo che sia possibile che qualcuno l'abbia aggiornato manualmente ma semplicemente non abbia importato il nuovo file di metadati che contiene il nuovo certificato in CUCM.

Se si verificano gli errori indicati:

- Se si utilizza AD FS, fare riferimento all'ID bug Cisco [CSCuj6703](#)
- Se NON si utilizza ADFS, raccogliere un nuovo file di metadati dall'IdP e importarlo in CUCM

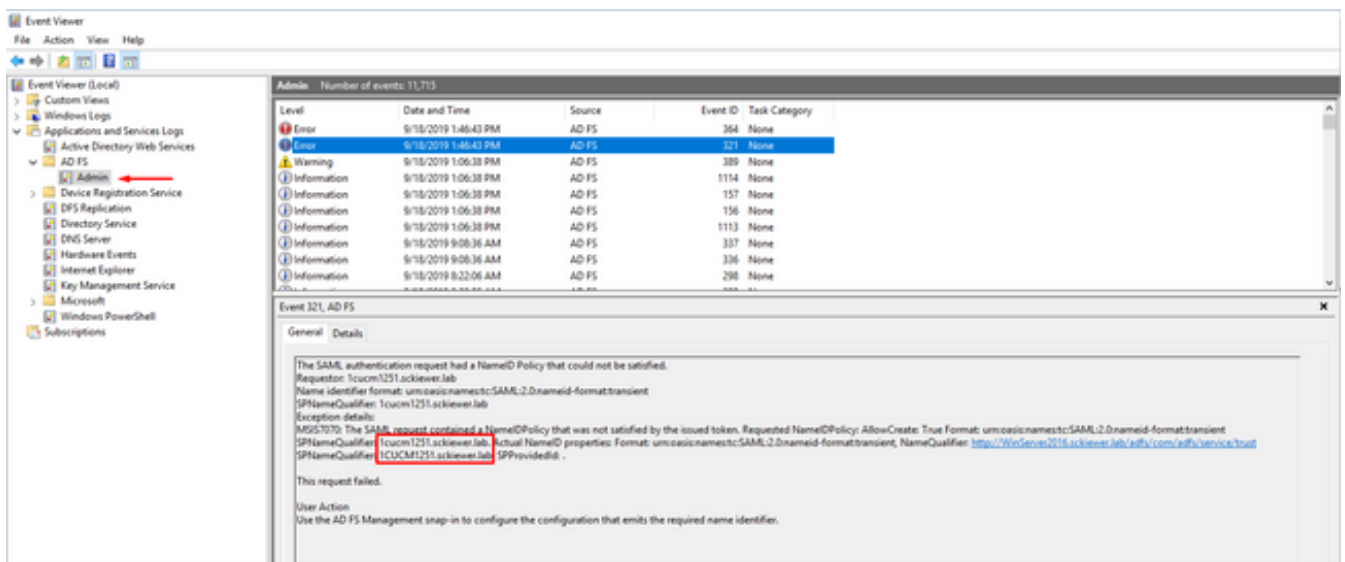
Codice di stato non valido nella risposta

Si tratta di un errore comune nelle distribuzioni con ADFS:

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

In quasi tutti i casi si tratta di un problema con la regola attestazione sul lato ADFS. Incollare prima la regola nel blocco note, aggiungere gli ID entità e quindi incollare la regola dal blocco note in AD FS. In alcuni casi, una copia/incolla direttamente dall'e-mail o dal browser può omettere alcuni segni di punteggiatura e causare un errore di sintassi.

Un altro problema comune è rappresentato dalla regola attestazione, ovvero il fatto che la combinazione di maiuscole e minuscole degli FQDN IdP o SP non corrisponde all'elemento entityID nei file di metadati. Controllare i registri del Visualizzatore eventi sul server di Windows per determinare se si tratta del problema.



Nell'immagine è possibile vedere che il valore di NameID richiesto è 1cucm1251.sckiewer.lab mentre il valore di NameID effettivo è 1CUCM1251.sckiewer.lab. Il NameID richiesto deve corrispondere all'entityID nel file di metadati SP mentre il NameID effettivo è impostato nella regola attestazione. Per risolvere il problema, è necessario aggiornare la regola di attestazione con un FQDN minuscolo per l'SP.

Stato SSO non corrispondente tra CLI e GUI

In alcuni casi, lo stato viene utilizzato e la GUI può mostrare informazioni diverse per quanto riguarda l'abilitazione o la disabilitazione dell'SSO. Il modo più semplice per risolvere il problema è disabilitare e riabilitare l'SSO. Poiché esistono diversi file e riferimenti che vengono aggiornati durante il processo di abilitazione, non è possibile provare ad aggiornare manualmente tutti questi file. Nella maggior parte dei casi, è possibile accedere alla GUI e disabilitarla e riabilitarla senza problemi. Tuttavia, è possibile visualizzare questo errore quando si cerca di accedere all'autore

tramite l'URL di ripristino o il collegamento principale:



HTTP Status 404 ? /ccmadmin/localauthlogin

type: Status Report

Message: /ccmadmin/localauthlogin

Description: http.404

È possibile controllare la GUI per vedere se l'URL di ripristino è un'opzione e controllare anche l'output dello stato degli utenti sso dalla CLI:

```
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
```

Quindi, controllare la tabella del nodo di processo. Nell'esempio riportato di seguito, è possibile notare che l'SSO è disabilitato nel database (vedere il valore tkssomode per 1cucm1251.sckiewer.lab all'estrema destra):

```
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

```

Per risolvere questo problema, impostare di nuovo il campo tkssomode della tabella dei nodi di processo su 2 in modo da poter accedere tramite l'URL di recupero:

```

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

```

A questo punto, verificare l'URL di ripristino e procedere con un'operazione Disable > Re-enable of SSO che attiva CUCM per aggiornare tutti i riferimenti nel sistema.

Informazioni correlate

- [Guida all'implementazione di SAML SSO per applicazioni Cisco Unified Communications, versione 12.5\(1\)](#)
- [Panoramica tecnica su SAML \(Security Assertion Markup Language\) V2.0](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).