

Risoluzione dei problemi di SSO in Cisco Unified Communications Manager

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Flusso di accesso in SSO](#)

[Decodifica risposta SAML](#)

[Log e comandi CLI](#)

[Problemi comuni](#)

[Difetti noti](#)

Introduzione

In questo documento viene descritto come configurare Single Sign-On (SSO) in Cisco Unified Communications Manager (CUCM).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- CUCM
- ADFS (Active Directory Federation Services)

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- CUCM 11.5.1.13900-52 (11.5.1SU2)
- ADFS 2.0

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.

Configurazione

Fare riferimento alla sezione Configurazione di Single Sign-On in CUCM.

- <https://www.cisco.com/c/en/us/support/docs/unified-communications/unified-communications-manager-version-105/118770-configure-cucm-00.html>
- <https://www.cisco.com/c/en/us/support/docs/unified-communications/unified-communications-manager-callmanager/211302-Configure-Single-Sign-On-using-CUCM-and.html>

Guida all'implementazione di SAML SSO per le applicazioni Cisco Unified Communications, versione 11.5(1).

- https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/SAML_SSO_deployment_guide/11_5_1/CUCM_BK_S12EF288_00_saml-ss0-deployment-guide--1151.html

SAML RFC 6596

- <https://tools.ietf.org/html/rfc6595>

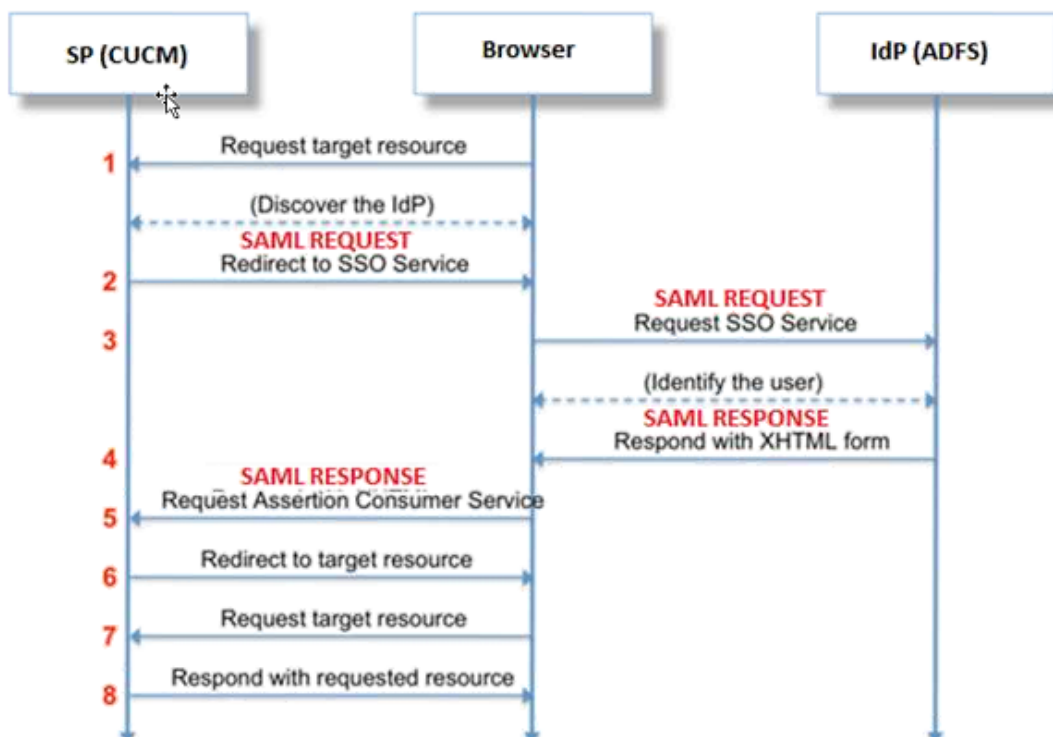
Verifica

Attualmente non è disponibile una procedura di verifica per questa configurazione.

Risoluzione dei problemi

Flusso di accesso in SSO

Authentication Flow



Decodifica risposta SAML

Utilizzo dei plug-in in Blocco note++

Installa questi plug-in:

```
Notepad++ Plugin -> MIME Tools--SAML DECODE
```

```
Notepad++ Plugin -> XML Tools -> Pretty Print(XML only - with line breaks)
```

Nei log SSO cercare la stringa "authentication.SAMLAuthenticator - SAML Response is ::" che contiene la risposta codificata.

Utilizzare questo plug-in o la decodifica SAML online per ottenere la risposta XML. La risposta può essere regolata in un formato leggibile con il plug-in Pretty Print installato.

Nella versione più recente di CUCM la risposta SAML è in formato XML, reperibile cercando "SPACSUtils.getResponse: risposta ottenuta=<samlp:

Risposta xmlns:samlp="e quindi stampare con il plug-in Pretty Print.

Utilizza Fiddler:

Questa utilità può essere utilizzata per ottenere il traffico in tempo reale e decodificarlo. Di seguito è riportata la guida per la stessa operazione: <https://www.techrepublic.com/blog/software-engineer/using-fiddler-to-debug-http/>.

Richiesta SAML:

```
ID="s24c2d07a125028bffffa7757ea85ab39462ae7751f" Version="2.0" IssueInstant="2017-07-15T11:48:26Z" Destination="https://win-91uhcn8tt3l.emeacucm.com/adfs/ls/" ForceAuthn="false" IsPassive="false" AssertionConsumerServiceIndex="0">
<saml:Issuer
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">cucmsso.emeacucm.com</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="cucmsso.emeacucm.com" AllowCreate="true"/>
</samlp:AuthnRequest>
```

Risposta SAML (non crittografata):

```
<samlp:Response ID="_53c5877a-0fff-4420-a929-1e94ce33120a" Version="2.0" IssueInstant="2017-07-01T16:50:59.105Z"
Destination="https://cucmsso.emeacucm.com:8443/ssosp/saml/SSO/alias/cucmsso.emeacucm.com"
Consent="urn:oasis:names:tc:SAML:2.0:consent:unspecified"
InResponseTo="s24c2d07a125028bffffa7757ea85ab39462ae7751f"
xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol">
<Issuer xmlns="urn:oasis:names:tc:SAML:2.0:assertion">http://win-91uhcn8tt3l.emeacucm.com/adfs/services/trust</Issuer>
<samlp:Status>
<samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success" />
```


</Assertion>

</samlp:Risposta>

Version="2.0" :- The version of SAML being used.

InResponseTo="s24c2d07a125028bffffa7757ea85ab39462ae7751f" :- The id for SAML Request to which this response corresponds to

samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success" :- Status Code of SAML response. In this case it is Success.

<Issuer>http://win-91uhcn8tt31.emeacucm.com/adfs/services/trust</Issuer> :- IdP FQDN

SPNameQualifier="cucmsso.emeacucm.com" :- Service Provider(CUCM) FQDN

Conditions NotBefore="2017-07-01T16:50:59.102Z" NotOnOrAfter="2017-07-01T17:50:59.102Z" :- Time range for which the session will be valid.

<AttributeValue>chandmis</AttributeValue> :- UserID entered during the login

Se la risposta SAML è crittografata, non sarà possibile visualizzare le informazioni complete e sarà necessario disattivare la crittografia su Intrusion Detection & Prevention (IDP) per visualizzare la risposta completa. I dettagli del certificato utilizzato per la crittografia si trovano in "ds:X509IssuerSerial" della risposta SAML.

Log e comandi CLI

Comandi CLI:

usa sso disable

Questo comando disabilita l'autenticazione basata su (OpenAM SSO o SAML SSO). Con questo comando vengono elencate le applicazioni Web per le quali è abilitato l'SSO. Quando richiesto, immettere **Sì** per disabilitare l'SSO per l'applicazione specificata. È necessario eseguire questo comando su entrambi i nodi se in un cluster. È inoltre possibile disabilitare l'SSO dall'interfaccia utente grafica (GUI) e selezionare il pulsante **Disabilita** in SSO specifico in Amministrazione Cisco Unity Connection.

Sintassi dei comandi

usa sso disable

utilizza stato sso

Questo comando visualizza lo stato e i parametri di configurazione di SAML SSO. Consente di verificare lo stato SSO, abilitato o disabilitato, su ogni singolo nodo.

Sintassi dei comandi

utilizza stato sso

utilizza sso enable

Questo comando restituisce un messaggio di testo informativo in cui viene richiesto all'amministratore di abilitare la funzione SSO solo dalla GUI. Impossibile abilitare con questo comando sia l'SSO basato su OpenAM che l'SSO basato su SAML.

Sintassi dei comandi
utilizza sso enable

utilizza sso recovery-url enable

Questo comando abilita la modalità SSO dell'URL di ripristino. Verifica inoltre che l'URL funzioni correttamente. È necessario eseguire questo comando su entrambi i nodi se in un cluster.

Sintassi dei comandi
utilizza sso recovery-url enable

utilizza sso recovery-url disable

Questo comando disabilita la modalità SSO dell'URL di ripristino in tale nodo. È necessario eseguire questo comando su entrambi i nodi se in un cluster.

Sintassi del comando
utilizza sso recovery-url disable

set samltrace level <livello traccia>

Questo comando abilita le tracce e i livelli di traccia specifici che possono individuare errori, debug, informazioni, avvisi o errori irreversibili. È necessario eseguire questo comando su entrambi i nodi se in un cluster.

Sintassi del comando
set samltrace level <livello traccia>

mostra livello samltrace

Questo comando visualizza il livello di log impostato per SAML SSO. È necessario eseguire questo comando su entrambi i nodi se in un cluster.

Sintassi del comando
mostra livello samltrace

Tracce per verificare il momento della risoluzione dei problemi:

Per impostazione predefinita, i log SSO non sono impostati su un livello dettagliato.

Eseguire prima il comando **set samltrace level debug** per impostare i livelli di log di cui eseguire il debug, riprodurre il problema e raccogliere i seguenti set di log.

Da RTMT:

Cisco Tomcat

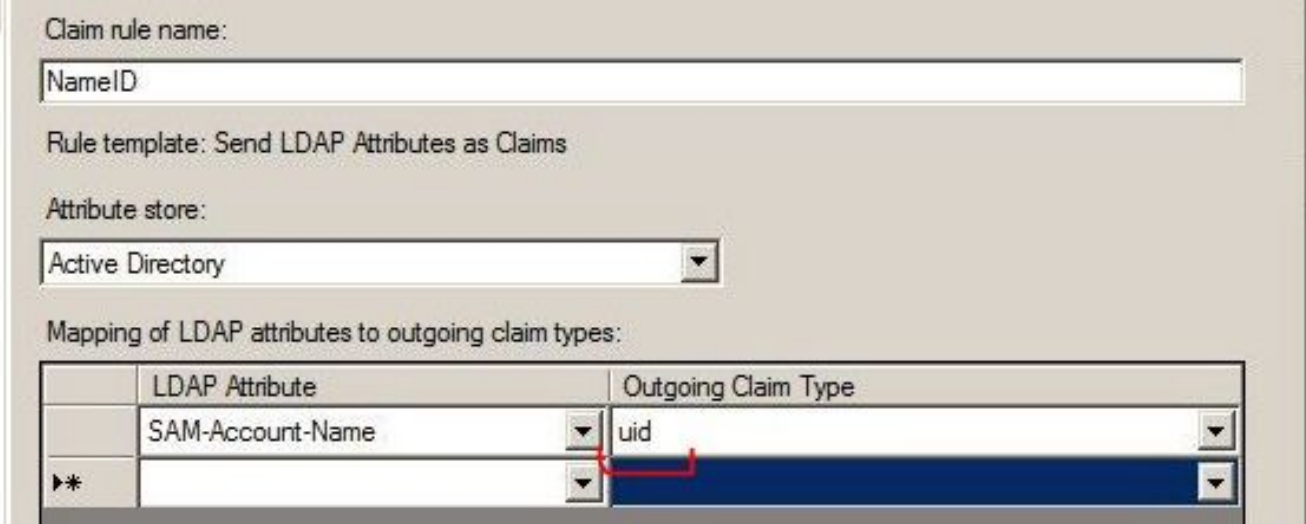
Cisco Tomcat Security

Cisco SSO

Problemi comuni

Valore non corretto per UID (Unique Identifier):

Dovrebbe essere esattamente UID e, in caso contrario, CUCM non è in grado di capirlo.



Claim rule name:
NameID

Rule template: Send LDAP Attributes as Claims

Attribute store:
Active Directory

Mapping of LDAP attributes to outgoing claim types:

	LDAP Attribute	Outgoing Claim Type
	SAM-Account-Name	uid
▶*		

Regola attestazione errata o criterio NameID errato:

È molto probabile che in questo scenario non vengano richiesti nome utente e password.

La risposta SAML non conterrà alcuna asserzione valida e il codice di stato sarà simile al seguente:

```
<samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:InvalidNameIDPolicy"/>
```

Verificare che la regola attestazione sia definita correttamente sul lato IDP.

Differenza tra maiuscole/minuscole definita nella regola attestazione:

L'FQDN CUCM nella regola attestazione deve corrispondere esattamente a quello specificato nel server effettivo.

È possibile confrontare la voce nel file xml dei metadati di IDP con quella presente in CUCM

eseguendo il comando **show network cluster/show network etho details** sulla CLI di CUCM.

Ora errata:

L'NTP tra CUCM e IDP presenta una differenza maggiore dei [3 secondi consentiti nella Guida alla distribuzione](#).

Firmatario asserzione non attendibile:

Al momento dello scambio dei metadati tra IDP e CUCM (provider di servizi).

I certificati vengono scambiati e, in caso di revoca del certificato, i metadati devono essere nuovamente scambiati.

Configurazione errata DNS/Nessuna configurazione

Il DNS è il requisito principale per il funzionamento dell'SSO. Eseguire il comando **show network etho detail**, **utilizzare il test di diagnosi** sulla CLI per verificare che DNS/Domain sia configurato correttamente.

Difetti noti

[CSCuj6703](#)

Il certificato di firma ADFS viene rinnovato e alle risposte IDP vengono aggiunti due certificati di firma alle risposte CUCM (SP), pertanto si verifica un errore. È necessario eliminare il certificato di firma non necessario

[CSCvf63462](#)

Quando si accede alla pagina SAML SSO da CCM Admin, viene visualizzato il messaggio "I seguenti server non sono riusciti durante il tentativo di ottenere lo stato SSO" seguito dal nome del nodo.

[CSCvf9678](#)

L'SSO basato su CTI non riesce quando si definisce il server CUCM come indirizzo IP in CCMAAdmin/System/Server.