

# Configurar e solucionar problemas de SSO no Cisco Unified Communications Manager (CUCM)

## Contents

---

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Círculo de Confiança](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configuração](#)

[Troubleshooting](#)

[Dados a Serem Coletados](#)

[Exemplo de análise](#)

[Informações do dispositivo do laboratório do TAC](#)

[Revisão de log para CUCM](#)

[Análise detalhada da solicitação e asserção SAML](#)

[Solicitação SAML](#)

[Asserção](#)

[Comandos CLI úteis](#)

[Alterar de AssertionConsumerServiceURL para AssertionConsumerServiceIndex](#)

[Problemas comuns](#)

[Não é Possível Acessar a Administração de SO ou a Recuperação de Desastres](#)

[Falha de NTP](#)

[Instrução de Atributo Inválida](#)

[Dois Certificados de Autenticação - AD FS](#)

[Código de Status inválido na Resposta](#)

[Incompatibilidade de status de SSO entre CLI e GUI](#)

[Informações Relacionadas](#)

---

## Introdução

Este documento descreve o recurso SSO no CUCM, a configuração, as dicas para solucionar problemas, a análise de log de exemplo e os recursos para obter informações adicionais.

## Pré-requisitos

### Requisitos

A Cisco recomenda o conhecimento de alguns termos de Logon Único (SSO):

- Security Assertion Markup Language (SAML) - um padrão aberto para trocar dados de autenticação e autorização entre as partes
- Provedor de serviços (SP) - O SP é a entidade que hospeda o serviço. Neste documento, o Cisco Unified Communications Manager (CUCM) é o provedor de serviços
- Provedor de Identidade (IdP) - O IdP é a entidade que autentica as credenciais do cliente. A autenticação é completamente transparente para o SP, de modo que as credenciais podem ser um cartão inteligente, nome de usuário/senha, etc. Depois que o IdP autentica as credenciais do cliente, ele gera uma asserção, a envia ao cliente e redireciona o cliente de volta ao SP
- Asserções - Uma informação sensível ao tempo que o IdP gera após a autenticação bem-sucedida de um usuário. A finalidade da asserção é fornecer informações sobre o usuário autenticado ao SP
- Ligações - define o método de transporte usado para entregar as mensagens do protocolo SAML entre entidades. Os produtos Cisco Unified Communications usam HTTP
- Perfis - restrições predefinidas e combinações de conteúdo de mensagens SAML (asserções, protocolos, vinculações) que funcionam para obter um caso de uso comercial específico. Este treinamento concentra-se no perfil de login único do navegador da Web, pois é o método usado pelo CUCM
- Metadados - conjunto de informações de configuração trocadas entre as partes. Contém informações como associações SAML com suporte, funções operacionais como IdP ou SP, atributos de identificador com suporte, informações de identificador e informações de certificado usadas para assinar e criptografar a solicitação ou resposta.

## Componentes Utilizados

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

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

## Informações de Apoio

A finalidade do SSO é permitir que usuários e administradores acessem vários aplicativos de colaboração da Cisco sem exigir autenticações separadas para cada um. A habilitação de SSO resulta em várias vantagens:

- Aumenta a produtividade porque os usuários não precisam inserir novamente as credenciais para a mesma identidade em produtos diferentes.
- Ele transfere a autenticação do sistema que hospeda os aplicativos para um sistema de terceiros. Você cria um círculo de confiança entre um IdP e um provedor de serviços que


permite que o IdP autentique usuários em nome do SP.

- Ele fornece criptografia para proteger as informações de autenticação passadas entre o IdP, o provedor de serviços e o usuário. O SSO também oculta as mensagens de autenticação passadas entre o IdP e o provedor de serviços de qualquer parte externa.
- Ele pode reduzir os custos à medida que menos chamadas ao help desk são feitas para redefinições de senha.

## Círculo de Confiança

Os certificados desempenham um papel muito importante no SSO e são trocados entre o SP e o IdP através de arquivos de metadados. O arquivo de metadados SP contém o certificado de criptografia e assinatura do provedor de serviços junto com algumas outras informações importantes, como os valores do índice de serviço de consumo de asserção e as informações de HTTP POST/REDIRECT. O arquivo de metadados do IdP contém seu(s) certificado(s) junto com algumas outras informações sobre os recursos do IdP. Você deve importar os metadados de SP para o IdP e importar os metadados de IdP para o SP para criar um círculo de confiança. Essencialmente, o SP assina e criptografa qualquer solicitação gerada com o certificado em que o IdP confia, e o IdP assina e criptografa qualquer asserção (resposta) gerada com certificados em que o SP confia.

---

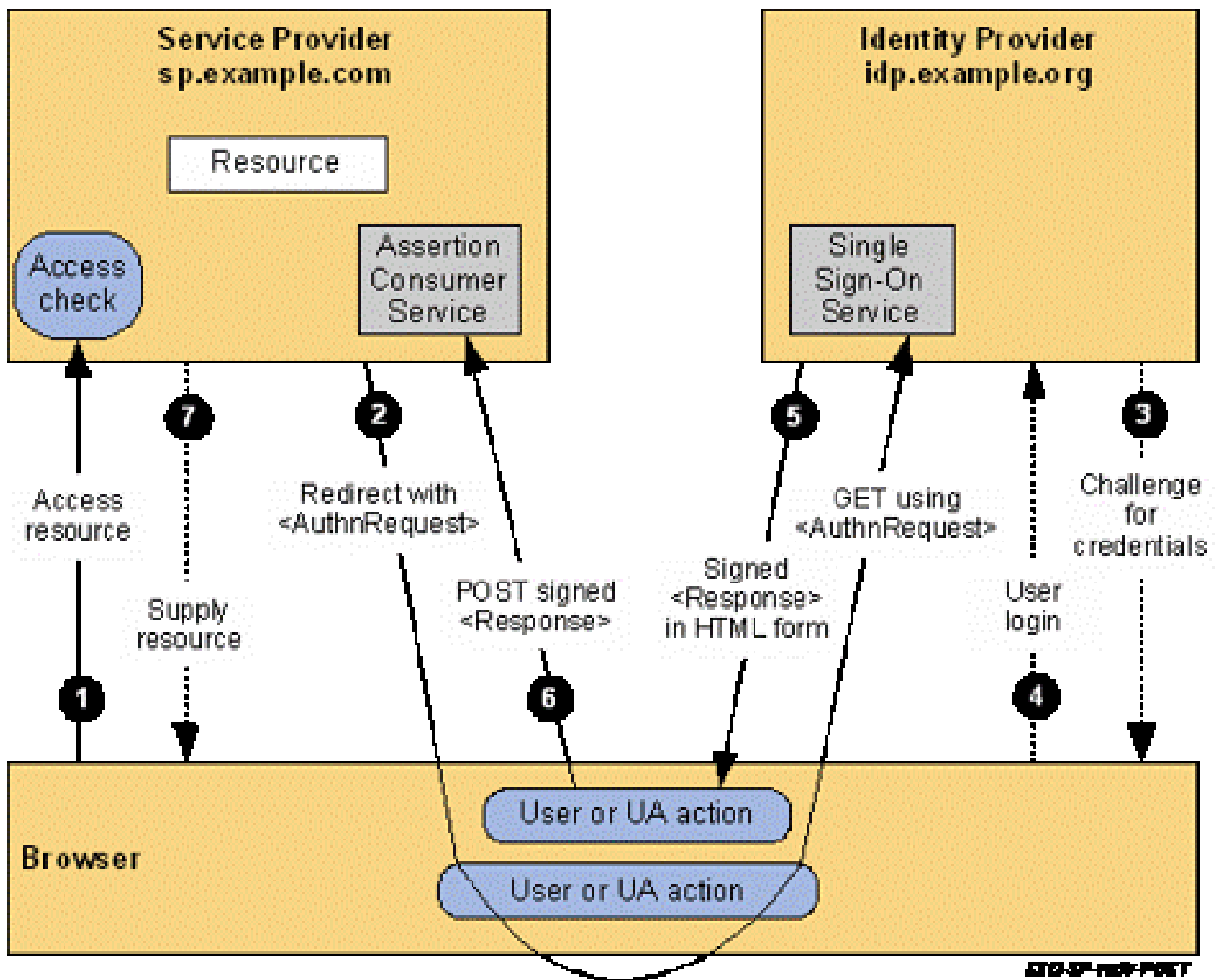
 Observação: se determinadas informações sobre a controladora forem alteradas, como o nome do host/Nome de domínio totalmente qualificado (FQDN) ou certificado de assinatura/criptografia (Tomcat ou ITRRecovery), o círculo de confiança poderá ser interrompido. Faça download de um novo arquivo de metadados do SP e importe-o para o IdP. Se determinadas informações sobre o IdP forem alteradas, baixe um novo arquivo de metadados do IdP e execute novamente o teste de SSO para que você possa atualizar as informações no SP. Se você não tiver certeza se sua alteração requer uma atualização de metadados no dispositivo oposto, é melhor atualizar o arquivo. Não há nenhuma desvantagem em relação a uma atualização de metadados em nenhum dos lados e essa é uma etapa válida para solucionar problemas de SSO, especialmente se houve uma alteração de configuração.

---

## Configurar

### Diagrama de Rede

O fluxo para um login SSO padrão é mostrado na imagem:



✎ Observação: o processo na imagem não está em ordem da esquerda para a direita. Lembre-se de que o SP é CUCM e o IdP é o aplicativo de terceiros.

## Configuração

Da perspectiva do CUCM, há muito pouco a ser configurado em relação ao SSO. No CUCM 11.5 e posterior, você pode selecionar SSO de cluster inteiro ou por nó.

- No CUCM 11.5, o SSO de todo o cluster requer que um certificado tomcat multiservidor seja instalado em todos os nós, já que há apenas um arquivo de metadados para todo o cluster (e o certificado é armazenado nesse arquivo, portanto cada nó deve ter o mesmo certificado tomcat).
- No CUCM 12.0 e posterior, você tem a opção de Usar certificado autoassinado gerado pelo sistema para SSO de todo o cluster. Esta opção usa o certificado ITLRecovery em vez de 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

- O SSO por nó é o padrão anterior ao CUCM 11.5. Em uma configuração por nó, cada nó tem seu próprio arquivo de metadados que precisa ser importado para o IdP, já que qualquer um desses nós pode potencialmente redirecionar um usuário para autenticação.
- Você também pode habilitar o SSO para RTMT no CUCM 11.5. Essa opção é ativada por padrão e está localizada em Cisco Unified CM Administration > Enterprise Parameters > Use SSO for RTMT.

 Observação: a observação que indica Se o modo SSO for Cluster Wide, o certificado Tomcat deve ser um certificado assinado por CA de vários servidores está incorreto nas versões 12.0 e 12.5 e um defeito foi aberto para corrigi-lo (ID de bug da Cisco CSCvr49382).


Além dessas opções, o restante da configuração do SSO está no IdP. As etapas de configuração podem variar consideravelmente com base no IdP escolhido. Estes documentos contêm etapas para configurar alguns dos IdPs mais comuns:

- [Guia de Configuração do Microsoft AD FS](#)
- [Guia de configuração do Okta](#)
- [Guia de configuração do PingFederate](#)
- [Guia de Configuração do Microsoft Azure](#)

## Troubleshooting

### Dados a Serem Coletados

Para solucionar um problema de SSO, defina os rastreamentos de SSO como debug. O nível de log do SSO não pode ser definido para depuração via GUI. Para definir o nível de log do SSO para depuração, execute este comando no CLI: `set samltrace level debug`

 Observação: esse comando não é Cluster wide, portanto ele precisa ser executado em cada nó que poderia estar envolvido com um log SSO na tentativa.

Depois que o nível de log tiver sido definido para depuração, reproduza o problema e colete esses dados do CUCM:

- Logs Cisco SSO
- Registros do Cisco Tomcat

A maioria dos problemas de SSO gera exceções ou erros nos logs de SSO, mas em algumas circunstâncias, os logs do Tomcat também podem ser úteis.

## Exemplo de análise

Informações do dispositivo do laboratório do TAC

CUCM (Provedor de serviços):

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

Windows Server 2016 (Provedor de Identidade):

- Serviços de Federação do Active Directory 3.0
- FQDN: WinServer2016.sckiewer.lab

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

```
%% 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 - SPACSUtills.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

```

## Análise detalhada da solicitação e asserção SAML

### Solicitação SAML

#### Análise e informações sobre a solicitação 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>

```

### Asserção

#### Análise e informações sobre a resposta 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>MIIC8DCCAdigAwIBAgIQQ2RhydXzTY1GQQ88eF3LWjANBgkqhkiG9w0BAQsFADAOMTIwMAYDVQQDEy1BREZ
</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) and

```

<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

```

## Comandos CLI úteis



- `utils sso disable` - Permite desabilitar o SSO se ele não estiver funcionando
- `utils sso status` - Mostra o status atual do SSO no nó
- `utils sso recovery-url enable` - Permite desabilitar o URL de recuperação
- `utils sso recovery-url disable` - Permite habilitar a URL de recuperação
- `show samltrace level` - Mostra o nível de log atual para logs SSO
- `set samltrace level` - Permite definir o nível de log para logs SSO. Isso precisa ser definido como `DEBUG` para que possamos solucionar problemas com eficiência.

## Alterar de `AssertionConsumerServiceURL` para `AssertionConsumerServiceIndex`

Quando o SSO de todo o cluster foi adicionado ao CUCM 11.5, o CUCM não grava mais a URL do `AssertionConsumerService` (ACS) na solicitação SAML. Em vez disso, o CUCM grava o `AssertionConsumerServiceIndex`. Veja estes trechos de uma solicitação SAML:

CUCM pré 11.5.1:

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

CUCM 11.5.1 e superiores:

```
AssertionConsumerServiceIndex="0"
```

Na versão 11.5 e posterior, o CUCM espera que o IdP use o número de índice ACS da solicitação para procurar o URL do ACS no arquivo de metadados que foi carregado durante o processo de configuração. Este trecho de metadados do CUCM mostra o URL do POST (do Publicador) associado ao índice 0:

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

Não há nenhuma solução alternativa para alterar esse comportamento e o IdP deve usar os valores do Índice ACS em vez da URL do ACS. Mais informações podem ser encontradas aqui, ID de bug Cisco CSCvc56596.

## Problemas comuns

### Não é Possível Acessar a Administração de SO ou a Recuperação de Desastres

No CUCM 12.x, os aplicativos da Web Cisco Unified OS Administration e Disaster Recovery System utilizam o SSO. Se as tentativas de login nesses aplicativos falharem com um erro 403

depois que você habilitar o SSO, é provável que a plataforma CUCM não consiga encontrar a ID de usuário. Isso ocorre porque esses aplicativos não fazem referência à tabela de usuário final usada pela Administração, Manutenção e Relatórios do CM. Por causa disso, a ID de usuário que o IdP autenticou não existe no lado da plataforma do CUCM, portanto, o CUCM retorna um 403 proibido. [Este documento](#) detalha como adicionar os usuários apropriados no sistema para que os aplicativos da plataforma usem o SSO com sucesso.

## Falha de NTP

O SSO diferencia tempo porque o IdP anexa um 'período de validade' às asserções. Para verificar se o tempo é o problema no seu caso, você pode procurar esta seção nos registros de 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 você encontrar `Time Valid?:false` em seus logs de SSO, investigue a seção Condições da asserção para identificar o período em que a asserção deve ser considerada válida:

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

Você pode ver no trecho de exemplo que essa asserção só é válida de 13:01:03:8917 a 14:01:03:8917 em 30/4/2021. Em um cenário de falha, consulte a hora em que o CUCM recebeu essa asserção e verifique se ela está dentro do período de validade da asserção. Se a hora em que o CUCM processou a asserção estiver fora do período de validade, essa é a causa do seu problema. Certifique-se de que o CUCM e o IdP sejam sincronizados com o mesmo servidor NTP, já que o SSO é muito sensível ao tempo.

## Instrução de Atributo Inválida

Consulte a análise da asserção [aqui](#) e veja a observação sobre a instrução do atributo. Os produtos Cisco Unified Communications exigem que uma declaração de atributo seja fornecida pelo IdP, mas às vezes o IdP não envia uma. Para referência, este é um `AttributeStatement` válido:

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

Se você vir uma asserção do IdP, mas a instrução de atributo for omitida, trabalhe com o fornecedor do software IdP para fazer as alterações necessárias para que ele forneça essa instrução. A correção difere com base no IdP e, em alguns cenários, mais informações podem ser enviadas nessa instrução do que você vê no snippet. Contanto que haja um Nome de atributo definido como uid e um Valor de atributo que corresponda a um usuário com os privilégios corretos no banco de dados CUCM, o login será bem-sucedido.

## Dois Certificados de Autenticação - AD FS

Este problema é específico do Microsoft AD FS. Quando o certificado de autenticação no AD FS está próximo da expiração, o Windows Server gera automaticamente um novo certificado, mas mantém o certificado antigo em vigor até que ele expire. Quando isso ocorre, os metadados do AD FS contêm dois certificados de assinatura. A mensagem de erro exibida quando você tenta executar o teste de SSO durante esse período é Erro ao processar a resposta SAML.



Nota: Um erro ao processar a resposta SAML também pode ser apresentado para outros problemas, portanto, não suponha que esse é o seu problema se você vir esse erro. Certifique-se de verificar os logs de SSO para verificar.

Se você vir esse erro, revise os logs de SSO e procure:

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

Esse erro indica que os metadados de IdP importados para o CUCM contêm um certificado de autenticação que não corresponde ao IdP usado nesse intercâmbio SAML. Este erro geralmente ocorre porque o AD FS tem dois certificados de assinatura. Quando o certificado original está próximo da expiração, o AD FS gera automaticamente um novo certificado. Você deve baixar um novo arquivo de metadados do AD FS, verificar se ele tem apenas um certificado de autenticação e criptografia e importá-lo para o CUCM. Outros IdPs também têm certificados de assinatura que precisam ser atualizados para que seja possível que alguém o atualize manualmente, mas simplesmente não tenha importado o novo arquivo de metadados que contém o novo certificado para o CUCM.

Se você encontrar os erros mencionados:

- Se você usar o AD FS, consulte a ID do Cisco Bug CSCuj66703
- Se você NÃO usar o AD FS, colete um novo arquivo de metadados do IdP e importe-o para o CUCM

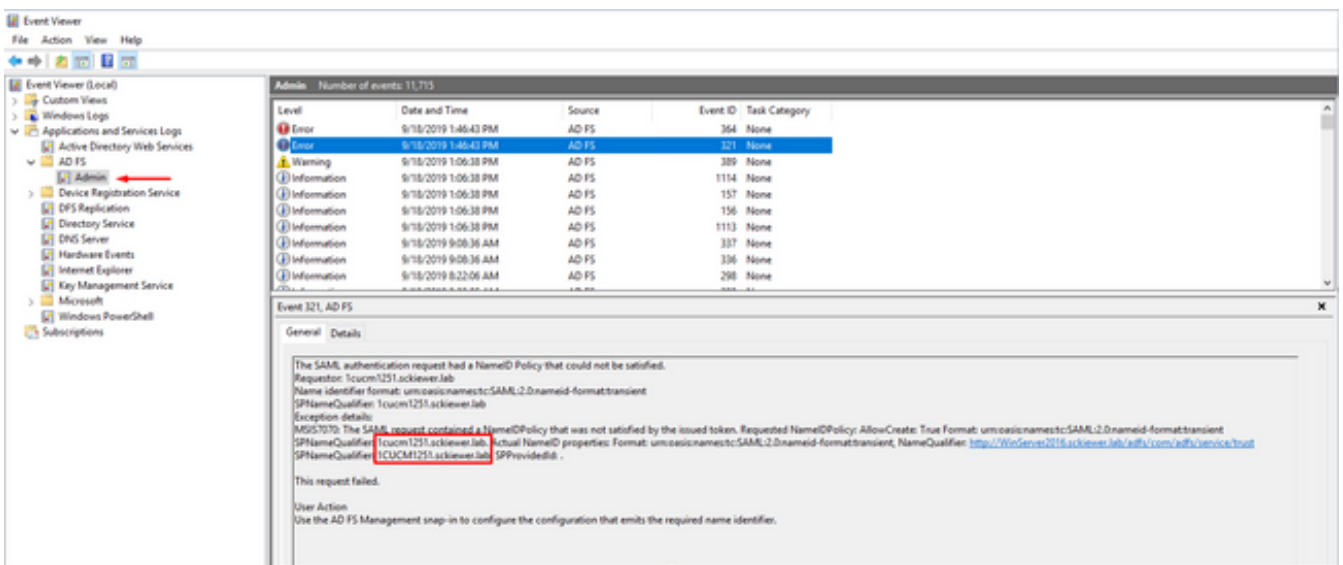
## Código de Status inválido na Resposta

Este é um erro comum em implantações com o AD FS:

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

Em quase todos os casos, isso é um problema com a regra de declaração no lado do AD FS. Cole a regra no bloco de notas primeiro, adicione suas entityIDs e cole a regra do bloco de notas no AD FS. Em alguns cenários, copiar/colar diretamente do seu e-mail ou navegador pode omitir alguns dos sinais e causar um erro de sintaxe.

Outro problema comum é com a regra de declaração que a capitalização do IdP ou dos FQDNs SP não corresponde ao entityID nos arquivos de metadados. Verifique os logs do Visualizador de Eventos no Windows Server para determinar se esse é o problema.



Você pode ver na imagem que o NameID solicitado é 1cucm1251.sckiewer.lab enquanto o NameID real é 1CUCM1251.sckiewer.lab. O NameID solicitado deve corresponder ao entityID no arquivo de metadados SP enquanto o NameID real estiver definido na regra de declaração. Para corrigir esse problema, preciso atualizar a regra de declaração com um FQDN minúsculo para o SP.

## Incompatibilidade de status de SSO entre CLI e GUI

Em alguns casos, os utils sso status e a GUI podem mostrar informações diferentes com relação à ativação ou desativação do SSO. A maneira mais fácil de corrigir isso é desabilitar e reabilitar o SSO. Existem alguns arquivos e referências que são atualizados por meio do processo de ativação, portanto, não é viável tentar atualizar manualmente todos esses arquivos. Na maioria dos casos, você pode fazer login na GUI e desativar e reativar sem problemas, no entanto, é possível ver este erro quando você tenta acessar o editor através da URL de recuperação ou do link principal:



## HTTP Status 404 ? /ccmadmin/localauthlogin

**type:** Status Report

**Message:** /ccmadmin/localauthlogin

**Description:** http.404

Você pode verificar a GUI para ver se o URL de recuperação é uma opção e também pode verificar a saída de `utils sso status` da 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
```

Em seguida, verifique a tabela do nó do processo. Neste exemplo, você pode ver que o SSO está desativado no banco de dados (consulte o valor `tkssomode` para `1cucm1251.sckiewer.lab` na extrema direita):

```
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 typossomode
enum name      moniker
==== =
0   Disable    SSO_MODE_DISABLE
```

- 1 Agent Flow SSO\_MODE\_AGENT\_FLOW
- 2 SAML SSO\_MODE\_SAML

Para corrigir isso, defina o campo tkssomode na tabela de nó de processo novamente como 2 para que você possa fazer logon por meio da URL de recuperação:

```
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

Nesse ponto, teste o URL de recuperação e continue com um Disable > Re-enable of SSO que acione o CUCM para atualizar todas as referências no sistema.

## Informações Relacionadas

- [Guia de implantação de SSO SAML para aplicativos Cisco Unified Communications, versão 12.5\(1\)](#)
- [Visão geral técnica da Security Assertion Markup Language \(SAML\) V2.0](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.