

فاشك تساو ليوختلا زمر حنم قفدت رشن لولح :ةقداصملا نيسحت - اهحالصاوه ئاطخأ 12.0 رادصإلا ، Cisco نم نواعتلا

تايوت حمللا

[ةمدقملا](#)

[ةيساسألا تابلطتملا](#)

[تابلطتملا](#)

[ةمدختسملا تانوكملا](#)

[ةيساسأ تامولعم](#)

[ةيسئيرلا ايازمللا](#)

[ةماه تارابتعا](#)

[ليوختلا دوك حنم قفدت رصانع](#)

[نيوكتلا](#)

[ةكبش ليل يطيختلا مسرلا](#)

[ةزيمملا زومرلا شيخت](#)

[ةزيمملا شيختلا زومرلا طاب](#)

[ةحصللا نم ققحتلا](#)

[اهحالصاوه ئاطخألا فاشك تساو](#)

[ةلص تاذا تامولعم](#)

ةمدقملا

شيخت ليل زيمملا زومرلا يلع ليوختلا زمر حنم قفدت دامتعا ةيفيك دنن تسمللا اذه حضوي ةزهجالا يلع Jabber ل ةصاخو ،ةفلتخملا ةزهجالا ربع Jabber مدختسم ةبرجت نيسحتلا ةلومحمللا .

ةيساسألا تابلطتملا

تابلطتملا

ةيلالاتلا عيضاوملاب ةفرعم كيديل نوكت نأب Cisco ي صوت

- Cisco Unified Communications Manager (CUCM)، 12.0 رادصإلا
- دحوملا لوخدلا (SSO)/SAML
- Cisco Jabber
- Microsoft ADFS ليغشتلا ماظن
- ةيوهلا رفوم (IDp)

ةيلالاتلا طباورلا يلع عجرا ،تاعوضوملا هذه لوح تامولعملا نم ديزم يلع لوصحلل

- [SAML SSO ل Cisco Unified Communications رشن ليل](#)
- [للاشم ليلكشت SAML SSO ل Cisco Unified Communications Manager](#)

جاتحي، لوصول اديج ازي م ازمري ليمع لانا كةرم لك يف. لصتم ريغ لوصول
فرعم المادختساب قداصلما ةداعا لىل مدختسمل

- لمعت مل. رشننلا ةي لمعل SSO نيكمت ةلاحي يف طقف ةزيمملا لوصول زومر رادصا مت
لىل ةزيمملا لوصول زومر مادختسا متي ملو ةلاحل هذه يف SSO فالخب رشننلا تاي لمع
تبات لكشب تاهجالا عيجم.
- مداخل ةركاذا يف ةظوفحم ىرألاب اهنكلو ايتاذ ةزيمملا Access زومر بظافتحال متي مل
ةطساوب هنم ققحتللا نكمي، لوصول زيمملا زمرا CUCM1 رصا اذا. اهرادصا ب ماق يذلا
CUCM2 لىل بجي يف، CUCM2 لىل ةمدخل لىل لوصول ليمعلا لواح اذا. طقف CUCM1
(ليكولا عضو) ةكبشل التاريخأت. CUCM1 لىل زيمملا زمرا اذه ةحص نم ققحتللا
هنأل ارظن ةيغلل ةئيس ةلومعلا ةلومحملا رتوي بملكلا ةزهجا عم مدختسمللا ةبرجت دعت
ةيمقر ةيدجبا حيتافم ةحول لىل دامتعالا تانايب لادعا مدختسمللا لىل نيعتي
ةعاس نم ةداع لمعي يذلا) مدختسمللا فرعم عم قداصلما ةداعا ب مدختسمللا موقوي ام دنع
(لماوع ةدع لىل فقوتي اذهو تا عاس 8 لىل ةدحاو).
- ظافتحال لىل ةددعتم تاهجاو ربع ةددعتم تاقيبطت لىل نوثدحتي نيذلا ءالمعلا جاتحي
نم نينثا نم لوخدلا ليحست سفل سلس معد دجوي ال. لتك/دامتعا تانايب ةدعب
نم لوخدلا ليحستب A مدختسمللا موقوي، لاثملا لىل بس لىل. نيلثامملا ءالمعلا
ةفلتخم iPhone فتاوه لىل لمعت يتل Jabber تاليتم.
- SSO فالخب رشننلا تاي لمعو SSO رشن تاي لمع نم لك معدل AuthZ.
- عم قفاوتم هنأل ارظنو. ليوختللا دوكنم قفدت + نيمضلا حنملا قفدت معدل AuthZ
اوملقا تي يتح لمعلا ةلصاومب RTMT لثم ءالمعلا حمسي هنإف، ةقباصل تارادصا لىل
زيمملا زمرا لوصول زيمملا زمرا AuthZ رصبي، ليوختللا دوكنم قفدت مادختساب
لوصول رخأ زيمملا زمرا لىل لوصلل شي دحتل زيمملا زمرا مادختسا نكمي. شي دحتل لىل
ةقداصل لىل ةجالا نود.
- زمر مدختستو ةرفشمو ةعقومو اهتاذب ةمئاق تادحو نع ةرابع يه ةزيمملا لوصول زومر
(RFC عم قفاوتم) يسايقلا (بيولا لىل زيمملا JSON زمرا) JWT.
- ماظن يف مداخل آل نكمي. ةعومجملا ماظن يف ةئيش ريفش تالو او عيقوتللا حيتافم
ةركاذلا لىل ةظفاحملا لىل ةجالا ال. لوصول زيمملا زمرا نم ققحتللا ةعومجملا
ةعومجملا يف ةيزكرملا ةقداصلما مداخل يه CUCM 12.0 لىل لمعت يتل ةمدخللا.
- ارداق لوؤسمللا نوكني نأ بجي. (DB) تانايبلا ةدعاق يف ةزيمملا شي دحتللا زومر نيزخت متي
مدختسمللا فرعم وأ مدختسمللا فرعم لىل لاطبالا دننسي. رمأل مزلا اذا، هلاطبا لىل
ليمعلا فرعمو.
- لوصول زومر نم ققحتللا ةفلتخملا تاجت نملل ةعقوملا ةزيمملا لوصول زومر حيتت
لمع تاقواو نيوكتلل لباقل لوصول زيمملا زمرا. اهنيزخت لىل ةجالا نود ةزيمملا
(يلاوتللا لىل اموي 60 و ةعاس 1 وه يضا رتفال) شي دحتل زيمملا زمرا
تامدخ عم لبق تسمللا يف رزاتللا هجاوب حمسي يذلا Spark عم JWT قيسنت ةادح متي
Spark Hybrid.
- A مدختسمللا نكمي eg: نيلثامم نيزاهج نم لوخدلا لىل جسي مدختسمللا سفلن معد
ةفلتخم iPhone فتاوه لىل لمعت يتل Jabber تاليتم نم لوخدلا ليحست

ليوختللا دوكنم قفدت رصانع

- Auth Z مداخل
- ريفش تاللا حيتافم
- عيقوتللا حيتافم
- ةزيمملا زومرلا شي دحت

نيوكتلا

يضا رتفا لكشب ةزيملا هذه نيكمت متي ال.

ةسسؤملا تاملعم > ماظن ىل لقتنا ،ةزيملا هذه نيكمتل 1. ةوطخلا

وه امك شيحتلل لوخدلا ليحست قفدت نيكمت عم مزحلل OAuth نييعتب مق 2. ةوطخلا ةروصلا يف حضورم.

SSO and OAuth Configuration		
OAuth Access Token Expiry Timer (minutes) *	<input type="text" value="60"/>	60
OAuth Refresh Token Expiry Timer (days) *	<input type="text" value="60"/>	60
Redirect URIs for Third Party SSO Client	<input type="text"/>	
SSO Login Behavior for iOS *	Use embedded browser (WebView)	Use embedded browser (WebView)
OAuth with Refresh Login Flow *	Enabled	Disabled
Use SSO for RTMT *	True	True

- يف عئاش ريفشتللو عيقوتلا حاتفم .هريفشتللو لوصولل زيمملا زمرلا عيقوت مت زمرلا ةحص نم ققحتلا ةوعومجملا ماظن يف ةدقع يأل نكمي هنا ينعي اذهو .ةوعومجملا ماظن لوصولل زيمملا .
- JWT (RFC 7519) قيسنتب دوجوم لوصولل زيمملا زمرلا .
- ةيحالص اءاتنا تقؤم) ةسسؤملا ةملعم مادختسا ةءاعاب ةزيمملا لوصولل زومر موقت زومرلا تاقيسنت نم لكل اهقيبطت متي يتلاو ،(OAuth ىل لوصولل زيمملا زمرلا ةديدللو ةميديلل ةزيمملا .
- ةقيد 60 - ةيضا رتفالا ةميقل .
- ةءحاو ةقيد - ةميقلل ىندألا دءلا .
- ةقيد 1440 - ةميقلل ىصقألا دءلا .

```
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpeGCI6IjkhMGQ1MzI0LWY0ZjAtNGIwYi04MTF1LlRlNTlmZGI2YjcyMjppZjMjY2E4MGJkZDdlZTM1ZDk3MDNiNjBiNTQ5MTBiZDQ0ODRiIn0.eyJwcm12YXR1IjoizXlKaGJHY2lPaUprYVhJaUxDSmpkSGtpT2lKSlYxUWlMQ0psYm1NaU9pSkJNVkE0UTBKRexVaFRNalUySWl3aWEybGtJam9pT0dRdlpEVXpNalF0WmpSbU1DMDBZakJpTFRneE1XVXROR0UxT1daa1lqWmlOek15T21Vd1ptUm1Zmk16WlRRMU5ERTFOV0ZpTkrJek5tRTJOMlV4T0RChU1qWmxZMk13WXpJeE56SX1OREJtWlRFellXWXlOak14TkRkalpHVXpNR1l3TjJJaWZRLi5xQWd6aGdRaTVMmKdlaDl5V2RvN25nLmdMTHNpaTRjQk50c1NEUXRjTE51RWRnWTl4WkVJvczJ4YzBaeTFGqjZQNmNzWWJfZkRnaDRZby04V1NaNjUzdXowbnFOalpXT1E1dGdnYW9qMlp6ZFk2ZzN2SWFHbF9JWUtNdkNIWNNscmt4YUFGTk5MWExLQlJmaTA2LVk2V3l1dUdxNmpNwk5DbnlKX1pTbUpkVFQwc1Z4RTdGTxVxaUJsME1rRGdyVDdvOFNXMEY5cXFadndEZDJSaDdqNkRjWGdks3VtOwltU2xNU1pjejhueVdic01Udk5yMWY0M25VenJzMHk5WNN6NnBDX0czZmlWYjJjSjVWLVFkcFh4TUo2bnZodXcydjRiUGVkm3VMQlpaVWl0Q3B6TUVDdW5NMlh1TVBrTGdlS1NqWG44aGhPRFNVcWlWQ0Uta3RZdnRbc2Q0RnJxcGNxWlZiS0ZiVTRbU0w2pMYVJtUk9IVl1QVkc0a3FBdTRWalVMUzVCRWszNnZ4Nmp3U3BMUy1IdTcwbVRNcmR3dmV5Q2ZOYkhyT0FlVmVvekFIR3JqdGhmaFpmSFVUTWZiNkMtX2tOQVJGQWdDclZTzy0wUz1xb1JvTWVkcUENETEE4MDJiaWwtNDJjOC15Mwo4X1FVaC02UUtCV2dodVd4VWtBODRpekFFaw1OQTlsSHFKM3Nxd2JFNURkZmhIay05bTJfTTN5Mw1wVkdorVQ3Zw9XVDBqWllnRGRBQjFzUGwxLTLasFNYYmsydTE3SkJVRV9FOXI0V0tWMnBqWgtiN0lQSWgtQ3JWQTZkcVdQRHVlbnx1V19wblNLYnYtTkZVbGQ0WEY3cmZLYmQySlg4eUhhX05pOVVVUnUwZVdsNwXGRUVabklubmFKZEdHLUZrb3VuN2xHSF1wSE4ydXVudmRnOHZVZzZsa0JPbmoz eUFjclZTMGxKc1NwdUxFLYldwd2c4YjdBdDM3d3AtMwT2Y1ZQaWpCQ11CV181d2JzbTFYd2k4MVC2WHVpNzZmZQVg3cEJVQnBfT2VRNzQ2ZXJjZkNUUFZCYUpZUGJuzWEtdFhsU3RmZzBGEVrmbnhnX1Vzazl3QXJkeme4c204T0FQaWMxZmFQOG0uUtDFN0FVX2xUVnNmZFI2bnkyUdhQsJ9.u2fJrVA55NQC3esPb4kcodt5rnjcl0-5uEDdUf-KnCYEPBZ7t2CTsMMVVE3nfrRhM39MfTlNS-qVOVpuoW_51NYaENXQMxfxlU9aXp944QiU10eFQKj_g-n2dEINRStbtUc3KMKqtz38BFf1g2Z51sdlnBn4XyVVPgGCf4XSfsFIa9ff051awQ0LcCv6YQTGer_6nk7t6F1MzPzBzZjala bpm--6LNSzjPftEiexpD2oXvW8V10Z9ggNk5Pn3Ne4RzqK09J9WChaJSXkTTE5G39EZcePmVntcbayq-L2pAK5weDa2k4uYmfAQAwcTOUrWk3yilwqjHAamG-CoipZQ
```

OAuth Refresh Token Expiry Timer" parameter in enterprise parameters page in CUCM.
 Path: System -> Enterprise parameters
 Values are integers ranging from 1 - 90
 Minimum lifetime = 1 Day
 Default lifetime = 60 days
 Maximum lifetime = 90 days

زيمم زمر ىلع لوصولل ليمعلا اهيف بلطي ةرم لك يف ديءج لوصولل زيمم زمر رادصا متي .

املاط احلاص مي دقلا لازي ال

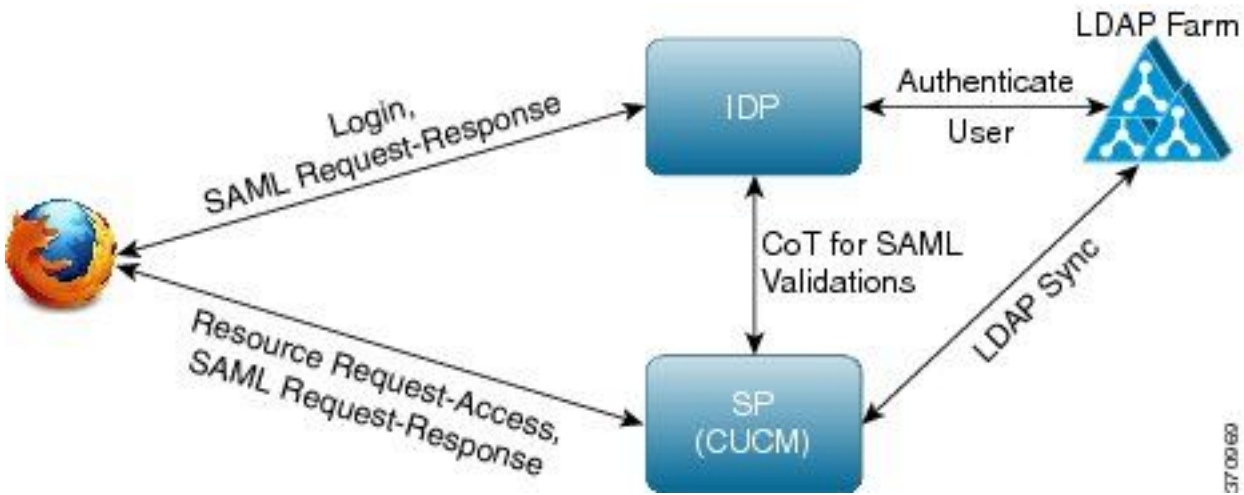
- ريفش التال اع قوتال حيتافم ريفيغت متي مل
- (زيمملا زمرلا لخاد عنزخملا) عي حالصلا لصاوف
- يهو، طاقن اهنيب لصفي، اعزجا ةثالث نم نوكتت: بيولا يل ع زيمملا JSON تادحو عي قوتال او ةلومحال او سارلا

لوصولل زيمملا زمرلا جذومن

- سارلا وه دوسالاب هزاربإ متي يذلا زيمملا زمرلا ةيادب في
- ةلومحال وه طسوال اعزجال
- عي قوتال وه ف قماعالاب ازربم زيمملا زمرلا ناك اذا، ةياهنلا في

ةكبش ل ل يطي طختال مسرلا

ينعمل تاملا كمالا قفدت يل ع يوتسملا ةيلاع ةماع ةرظن يل ي امي في



ةزيمملا زومرلا شي دحت

- شي دحتل زيمملا زمرلا عي قوت مت
- تانايبلا ةدعاق في RefreshTokenDetails لودج في شي دحتل زيمملا زمرلا نيزخت متي ةدعاق ةطساوب لثامتملا خس نلا عنم وه اذه نم ضرغلا. اهب ةصاخ ةئزجت ةمي قك هلي غشت كنكمي لودجال ةعجارمل. هرايتخاب ام صخش موقوي نا كنمي شي تانايبلا

```
run sql select * from refreshtokendetails
```

ةعارقلل لباق ةي حالص خيراتب وأ

```
run sql select pkid,refreshtokenindex,userid,clientid,dbinfo('utc_to_datetime',validity) as validity,state from refreshtokendetails
```

```
admin:run sql select * from refreshtokendetails
```

pkid	refreshtokenindex	userid	clientid	validity	state
173e2283-1...	65483476618891...	bvanturn	Clb4b...	2019-01-05 14:11:46	1080686546
cd2c634c-7...	0bf6b2989db114...	bvanturn	Clb4b...	2019-01-05 14:28:41	569144456
a3706858-b...	b4800f20dbfe0e...	bvanturn	Clb4b...	2019-01-05 14:38:12	1146722445

ةي حالص اهاهتنا دن تانايبلا ةدعاق نم شي دحتل زيمملا زمرلا حسم متي ري دحت كنمي ال) ايموي احابص ةيناثلا في تقوملا طبارت رشوم لغيشت متي. ةي حالصلا (دعب نع معدلا باسح لالخ نم هلي دعت كنمي نكلو، مدختسملا ةهجاو لالخ نم هنيوكت حلص ريغ زومرلا هذه نإف، ةزيمملا لوصولل زومر نم ريبك ددع يل ع يوتحي لودجال ناك

Certificate Details(Self-signed) - Internet Explorer provided by Cisco Systems, Inc.

https://10.77.29.184/cmplatform/certificateEdit.do?cert=/usr/local/platform/.security/authz/certs/authz.j Certificate error

Certificate Details for AUTHZ_CUCM-184, authz

Regenerate Download .PEM File Download .DER File

Status

Status: Ready

Certificate Settings

File Name	authz.pem
Certificate Purpose	authz
Certificate Type	certs
Certificate Group	product-cpi
Description(friendly name)	Self-signed certificate generated by system

Certificate File Data

```
[
[
Version: V3
Subject: L=i, ST=i, CN=AUTHZ_CUCM-184, OU=i, O=i, C=IN
Signature Algorithm: SHA256withRSA, OID = 1.2.840.113549.1.1.11

Key: CiscoJ RSA Public Key, 2048 bits
modulus:
310088952412132774650041525392629167237879710935753621934671843
216346326898490353644164813514840735197164588955185219996734516
256663568507413849247845292675452179850077675141884383314726763
520023902784651553941826511494962731151521090167892375623419501
739811988911210916820812069748957615302991414362015465824669063
319779866264424936428249029193098223306846888723560182717860238
318402233050626785154245146789308145325775236137097363983609689
```

Regenerate Download .PEM File Download .DER File

ةوصوللا يف حضوم وه امك CLI رمأ مادختساب Authz عيقوت حاتفم ةداعتسا متي.

```
CUCM-184 login: admin
Password:
Last login: Tue Nov 15 15:43:52 on tty1
Command Line Interface is starting up, please wait ...
```

Welcome to the Platform Command Line Interface

```
VMware Installation:
 1 vCPU: Intel(R) Xeon(R) CPU E5-2643 0 @ 3.30GHz
Disk 1: 80GB, Partitions aligned
6144 Mbytes RAM
```

```
admin:set ke
admin:set key regen authz signing
```

```
WARNING: This operation will regenerate the Authorization Service signing key and restart the Authorization Service on all the nodes. It is recommend that this command be run off-hours to avoid end user impact.
```

```
Proceed with regeneration (yes/no)? yes
```

```
signing key for the Authorization service generated succesfully.
```

```
admin:_
```

تتميزت بواجهة CLI مدمجة مع واجهة إيفيوتل حيث أفهم وضع لؤوسم لل نكمي
يصل الواجهات لل نم الدب حات للم.

وهو حيث أفهم ال وضع ب صاخال رمأل

ة.روصل اليف حضورم وه امك وحات للم ايفيوتل راهظا: عيفيوتل حات للم

```
admin:show key authz signing
authz signing key with checksum: a155d81be734850226f990a62816f1ae last synced on: 06/09/2017 13:04:47
```

ة.روصل اليف حضورم وه امك و show key authz encryption: ريفيوتل حات للم

```
admin:show key authz encryption
authz encryption key with checksum: 88edce92173e33f9cedbbfb09cd0e8c4 last synced on: 06/14/2017 16:22:06
```

ن.يفللتخم ريفيوتل ايفيوتل اة قداصم نم لك نوكي ام امئاد: اةظالم

ةحصل ال نم ققحتل

حيحصل لكشب نيوتل للمع ديكأتل مسقلا اذه مدختسا

ةكبشال لؤوسم يلع بجي، Cisco Unity Connection (CUC) مداخل يلع OAuth مداخلتسا | داري ام دنع
ن.يتوطخ ذي فننت

حياتافم وزي مالم OAuth زمر عيفيوتل بلجل Unity Connection مداخل نيوتل ب مق 1. ةوطخال
للم ريفيوتل CUCM.

CUC مداخل يلع OAuth تامدخ نيكم تب مق 2. ةوطخال

لي صافات م ادختساب ة دحولا ني وكت بجي ، ريفش تال او عيقوتال احي تافم بلجل : ةظحال م مدع ةلاح يف CUCM AXL لى لوصولل هني كمت مت مدختسم باسحو CUCM فيضم ريفوت نكمي الو CUCM نم زي ممل OAuth زمر دادرتسا Unity م داخ لىل ع رذعتي ، اذه ني وكت ني م دختسم لىل يتوصلال ديربالا لوخد لىل جس .

Authz مداوخ > ماظنلا تاداع | Cisco Unity Connection Administration > قراد | لىل لوقت نا

New Authz Server

Authz Servers Reset Help

Save

New Authz Server

Display Name* Authz Server

Authz Server* CUCMPublisher.miguecas.lv

Port* 8443

Username* miguecas

Password*

Ignore Certificate Errors

Save

Fields marked with an asterisk (*) are required.

اهحال صا و ااطخال فاشكتسا

اهحال صا و ني وكتال ااطخال فاشكتسال اهم ادختسا كنكمي يتال تامول عمل مسقلا اذه رفوي .

عجار ، لوخدلا لىل جس Cisco Jabber في مدختسم لىل ع رذعتو OAuth م ادختسا مت اذا : ةظحال م ادع Instant Messaging و Presence و CUCM مداوخ نم ريفش تال او عيقوتال احي تافم امئاد (IM&P).

IM&P و CUCM دقع عي مچ لىل ع ني رمالا نيذه لي غشت لىل ةكبشال ولوؤسم جاتحي

- جاتفملا ةقداصم عيقوت راهظا |
- show key authz encryption

ةداع بلطتت اهناف ، دقع ال عي مچ ربع ريفش تال او عيقوتال ةقداصم تاجرم قباطت مل اذا IM&P و CUCM دقع عي مچ لىل ع ني رمالا نيذه لي غشت مزلي ، كلذ ذي فننل . عاشنالا

- جاتفملا عجرم ريفش ني عت
- جاتفملا عجرم عيقوت ني عت

دقع ال عي مچ لىل ع Cisco Tomcat ةمدخ لي غشت ةداع مزلي ، كلذ دع

Cisco Jabber تالجس لىل ع اذه اطلال رطس لىل ع روثلال نكمي ، احي تافملا قباطت مدع عم

from refresh token, maybe server issue.

عقواوملا هذه في SSO قيبطت تالجس عاشنإ متي

- عومجمل عبتت نيوكت ي اذه بلطتي ال platform/log/ssoApp.log فلملا ضرع ةي لمع تالخدإ عاشنإ متي، SSO قيبطت ةي لمع ذيفنت اهيف متي ةرم لك في .تالجسلا ssoApp.log فلم في ةديج لجس
- ActiveModel/log/ssosp/log4j تالفلملا ةمئاق: SSOSP تالجس ،مساب عقوملا اذه في ديديج لجس فلم عاشنإ متي، SSO نيكم متي ةرم لك في تاي لمع لك وىرخأ SSO ةي لمع يأل فلملا اذه لوخد ليجست متي امك .ssosp00xx.log OAUTH.
- /log/certMgmt*.log يساسألا ماظنلا طاشن تالفلملا ةمئاق: تاداهشلا تالجس ديديج لجس فلم عاشنإ متي، (UI و CLI) AuthZ ةداهش عاشنإ اهيف متي ةرم لك في .ثدحل اذهل .ثدحل اذهل ديديج لجس فلم عاشنإ متي، Authz ري فشت حاتفم عاشنإ ةداعإل

ةلص تاذا تاملعم

[12.0 رادصلال Cisco نم نواعتلال لجم OAuth رشن](#)

ةمچرتل هذه لوج

ةللأل تاي نقتل نمة ومة مادختساب دن تسمل اذة Cisco تمةرت
ملاعلاء انء مء مء نمة دختسمل معد و تمة مء دقتل ةر شبل او
امك ةق قء نوك ت نل ةللأل ةمچرت لصف أن ةظحال مء ءرء. ةصاأل مء تءل ب
Cisco ةللخت. فرتمة مچرت مء دقء ةللأل ةفارتحال ةمچرتل عم لاعل او
ىل إأمءءاد ءوچرلاب ةصوء و تامچرتل هذه ةقء نء اهءل وئس م Cisco
Systems (رفوتم طبارل) ةلصلأل ةزءل ءن إل دن تسمل