

# هجاو ىل لودل لىجست عااأ فاشكتسا ISE 3.1 ل (GUI) ةيموسرلا مدختسملا SAML SSO مادختساب اءالساو

## تاىوتءملا

[ءمدقملا](#)

[ءىساسألا تابلطتملا](#)

[تابلطتملا](#)

[ءمدختسملا تانوكملا](#)

[عااألا ءىءصت نىءم](#)

[تالءسلا لىزن](#)

[لوصولا ضفرم: 1a ءلكشملا](#)

[لءل/للسلا](#)

[\(لوصولا ضفرم\) SAML ءباءتسا لى ءءءتم تاعومءم: 1b ءلكشملا](#)

[404 دروم لىل عروءءلا مءىمل: 2 ءلكشملا](#)

[لءل/للسلا](#)

[ءءاهشلا رىءء: 3 ءلكشملا](#)

[لءل/للسلا](#)

## ءمدقملا

لألء نم SAML ل (GUI) ةيموسرلا مدختسملا هجاو ىل لودل لىجست عم ISE 3.1 لى اهءطءالم مءىءل لءلءملا مءعم ءنءسملا اءه فصى ةىوه رفوم لى مادءتسا كنىمى. ISE لى (SSO) لىءال لودل لىجست ةىءناكم SAML لى ءنءسملا لوؤسملا لءء فىضى، SAML 2.0 راءى عم مادءتسا ءىوه رفوم لى مادءتسا كنىمى. ISE لى (SSO) لىءال لودل لىجست ةىءناكم SAML لى ءنءسملا لوؤسملا لءء فىضى، SAML 2.0 قبىطى P فرعم لىءا وءل ءرابع وءل PingOne وءل OKTA وءل Azure لءم (IDP).

## ءىساسألا تابلطتملا

### تابلطتملا

ءىءلءال عىضاوملاب ءفرعم كىءل نوكء ناب Cisco لىصوء:

1. لىءل وءل Cisco ISE 3.1

2. SAML SSO Setups تاءىساسألا مءهف

لوح لىصافءالا نم ءىزم لىل لوصءل لىءل [Azure AD عم SAML رءب](#) لىءل [ISE لوؤسم لودل لىجست قءءءو](#) وءل [SAML نىءوكءل ISE 3.1 لوؤسم لىءل](#) لىءل عءرا قءءءالا وءل نىءوكءالا.

ءءافءل لمءء اءنا نم ءكأءو، ءىوهلا ءوزم ءمدءب ءىءل نوكء ناب لىءى: **ءطءالم**

## ءمدختسملا تانوكملا

ءىءلءال ءىءاملا تانوكملا وءل ءمءرءل تاراءى لىءل ءنءسملا اءه لىءل ءءراولا تامولءملا ءنءست

• ISE 3.1 راءىءل

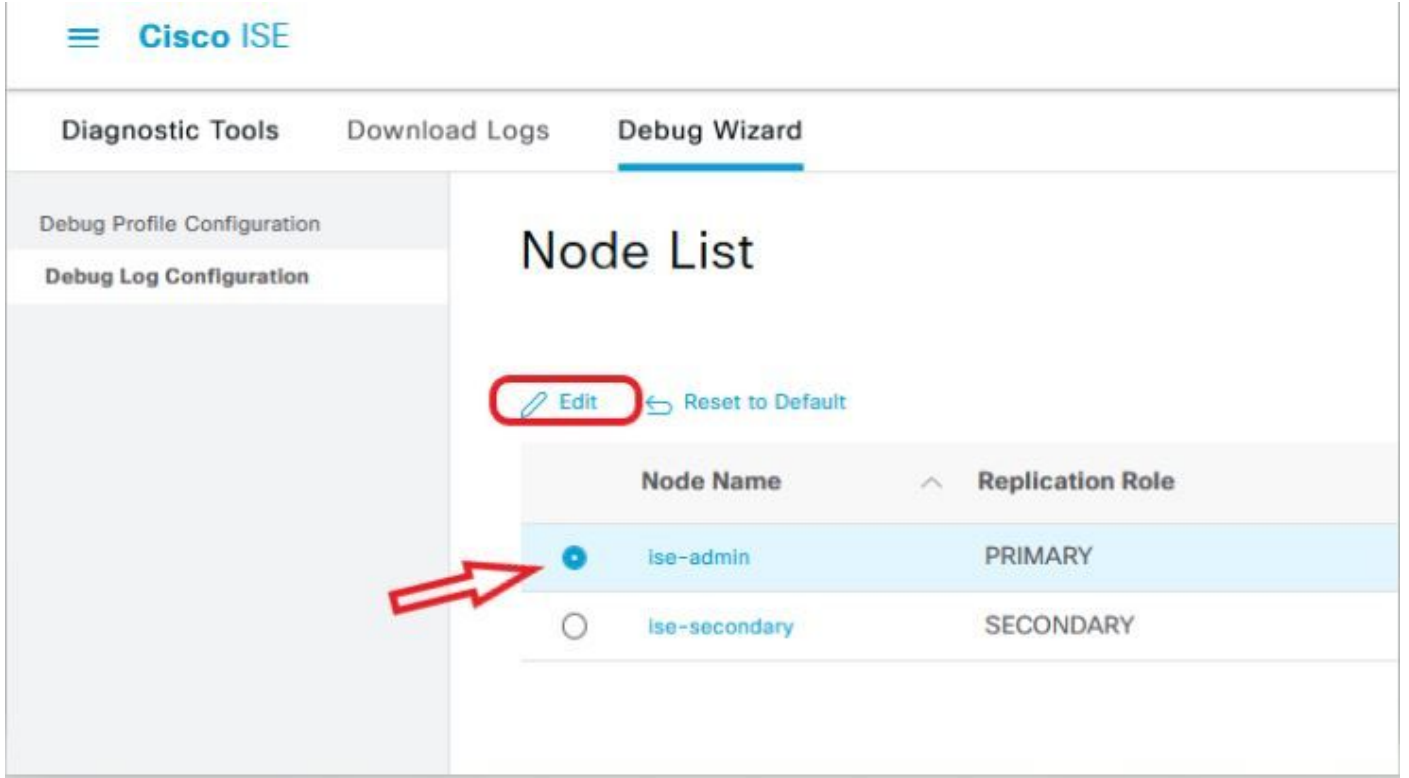
ءصاء ءىلمعم ءىءب لىءل ءءوءوملا ءهءال نم ءنءسملا اءه لىءل ءءراولا تامولءملا ءاشءنءم

تتأكد إذا (يضايرت فإ) حوسم نيوكتب دن تسمل اذ ه ي ف م دخت سمل ةزه ج أا عي مج ت أدب رم أ ي أ ل م ت ح م ل ر ي ث أ ت ل ل ك م ه ف ن م د ك أ ت ف ، ل ي غ ش ت ل ا د ي ق ك ت ك ب ش

## ءاطخ أا ح ي ح ص ت ن ي ك م ت

ح ض و م و ه ا م ك ءاطخ أا ح ي ح ص ت ت ا ي ل م ع ن ي ك م ت ا ل و أ ب ج ي ، ا ه ا ل ص ا و ءاطخ أا ف ا ش ك ت س أ ء د ب ل ه ا ن د أ .

ر ي ر ح ت ي ل ع ر ق ن ا و ة س ا س ا ل ا ة ر ا د ا ل ا ة د ق ع د ح . ءاطخ أا ل ج س ن ي و ك ت > ءاطخ أا ح ي ح ص ت ج ل ا ع م > ا ه ا ل ص ا و ءاطخ أا ف ا ش ك ت س أ > ت ا ي ل م ع ل ا ي ل ل ق ت ن ا ة . ل ل ا ت ل ا ة ر و ص ل ا ي ف ح ض و م و ه ا م ك



- ءاطخ أا ح ي ح ص ت ي و ت س م ي ل ع ة ل ل ا ت ل ا ت ا ن و ك م ل ن ي ي ع ت ب م ق

ن و ك م ل م س ا	ل ي ج س ت ل ا ي و ت س م	ل ج س ل ا ف ل م م س ا
ء ب ا و ب	ءاطخ أا ح ي ح ص ت	guest.log
ل م ا س ن ب و أ	ءاطخ أا ح ي ح ص ت	ise-psc.log
ل م ا س	ءاطخ أا ح ي ح ص ت	ise-psc.log

ء ا ع ا " ق و ف ر ق ن ا و ة د ق ع ل ا د ي د ح ت ق ي ر ط ن ع ءاطخ أا ح ي ح ص ت ن ي ي ع ت ة د ا ع ا ر ك ذ ت ، ا ه ا ل ص ا و ءاطخ أا ف ا ش ك ت س أ ن م ا ه ا ت ن ا ل ا د ن ع : ة ط ح ا ل م " . ي ض ا ر ت ف ا ل ا ي ل ل ن ي ي ع ت ل ا

## ت ا ل ج س ل ل ي ز ن ت

ء ي ر و ر ض ل ا ل ج س ل ا ت ا ف ل م ي ل ع ل و و ص ح ل ا ك ي ل ع ب ج ي ، ة ل ك ش م ل ا خ س ن م ت ي ن ا د ر ج م ب

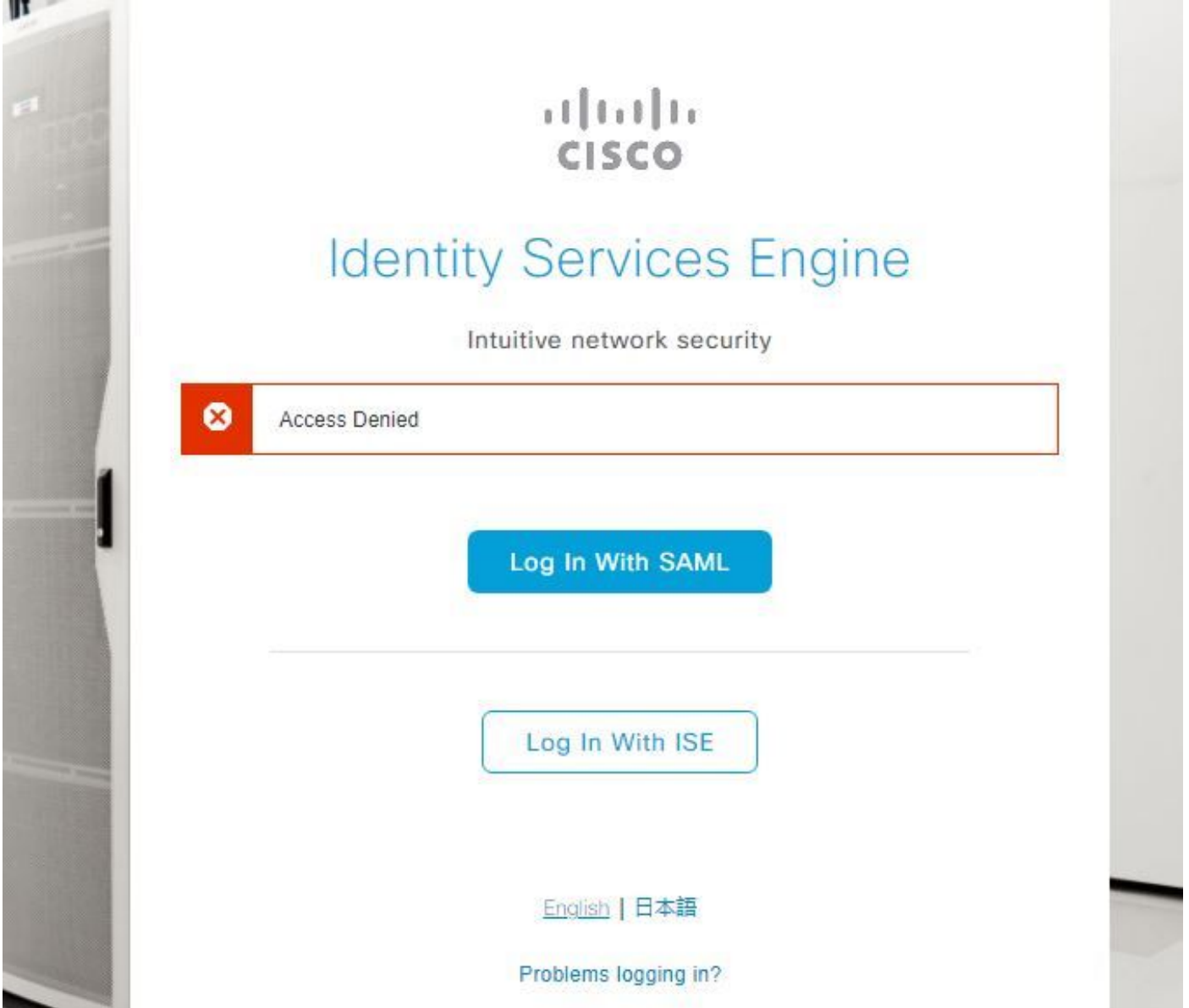
ت ا ل ج س > ' ز ا ه ج ل د ق ع ة م ئ ا ق ' ن م ض ة س ا س ا ل ل و و س م ل ا ة د ق ع د ح . ل ي ز ن ت ل ا ت ا ل ج س > ا ه ا ل ص ا و ءاطخ أا ف ا ش ك ت س أ > ت ا ي ل م ع ل ا ي ل ل ق ت ن ا . 1 ة و ط خ ل ا ءاطخ أا ح ي ح ص ت

ء ا ل ج س ل ل ISE-PSC و ف ي ض ل ل ل ص ا ل ا ت ا د ل ج م ل ا د م و ن ا م د ح . 2 ة و ط خ ل ا

ت ا ف ل م lse-psc.log و guest.log ل ي ز ن ت . 3 ة و ط خ ل ا

## لوصول اضف فرمت 1a: ةلكشمال

- SAML، إلى دن تسمال لوؤسمال لوخذ ليجست نيوكت دع ب
- SAML مادختساب لوخذل ليجست ددح
- عقوم وه امك IdP إلى لوخذل ليجست ةحفصل لمع إلى هيجوتلال ةداعال
- ةباجتسال ل لك ةحجان ةقداصمال دع ت SAML/IdP
- ISE في نوكمال نئالكال/ةومجمال فرعم سفن ةيؤركنكمي و IdP لاسرا ةعومجم ةمس
- ةطلق في حضوم وه امك، "لوصول اضفر" ةلاس رووظ في ببستي ءانثتسال يمر ب موق ي هناف، هتاسايس ليجت ISE لواحي امن ي ب، م ث، ةشاشال



### ise-psc.log في لوخذل لچس

```
2021-09-27 17:16:18,211 DEBUG [https-jsse-nio-10.200.50.44-8443-exec-2][  
cpm.saml.framework.impl.SAMLFacadeImpl -::::- AuthenticatePortalUser - Session:null IDPResponse:  
IdP ID: TSDLAB_DAG Subject: ise.test Group: null SAML Status  
Code:urn:oasis:names:tc:SAML:2.0:status:Success SAML Success:true SAML Status Message:null SAML  
email: SAML Exception:nullUserRole : NONE 2021-09-27 17:16:18,218 DEBUG [https-jsse-nio-  
10.200.50.44-8443-exec-2][ cpm.saml.framework.impl.SAMLFacadeImpl -::::- AuthenticatePortalUser  
- about to call authenticateSAMLUser messageCode:null subject: ise.test 2021-09-27 17:16:18,225  
DEBUG [https-jsse-nio-10.200.50.44-8443-exec-2][ cpm.saml.framework.impl.SAMLFacadeImpl -::::-  
Authenticate SAML User - result:PASSED 2021-09-27 17:16:18,390 INFO [admin-http-pool5][  
ise.rbac.evaluator.impl.MenuPermissionEvaluatorImpl -::::- *****Rbac Log  
Summary for user samlUser***** 2021-09-27 17:16:18,392 INFO [admin-http-
```

```

pool5][[] com.cisco.ise.util.RBACUtil -::::- Populating cache for external to internal group
linkage. 2021-09-27 17:16:18,402 ERROR [admin-http-pool5][[]
cpm.admin.infra.utils.PermissionEvaluationUtil -::::- Exception in login action
java.lang.NullPointerException 2021-09-27 17:16:18,402 INFO [admin-http-pool5][[]
cpm.admin.infra.action.LoginAction -::::- In Login Action user has Menu Permission: false 2021-
09-27 17:16:18,402 INFO [admin-http-pool5][[] cpm.admin.infra.action.LoginAction -::::- In Login
action, user has no menu permission 2021-09-27 17:16:18,402 ERROR [admin-http-pool5][[]
cpm.admin.infra.action.LoginAction -::::- Can't save locale. loginSuccess: false 2021-09-27
17:16:18,402 INFO [admin-http-pool5][[] cpm.admin.infra.action.LoginActionResultHandler -::::-
Redirected to: /admin/login.jsp?mid=access_denied

```

## لحل/البسلا

ISE في هنيوكت مت يذلا هسفن وه IdP تانويوكت في ةومجملا ةبلاطم مسا أن نم دكأت

Azure بنج نم ةشاشلا ةطوقل طاقنلا مت

Microsoft Azure Search resources, services, and

Home > Enterprise applications | All applications > [Redacted] SAML-based Sign-on > SAML-based Sign-on >

### Attributes & Claims

+ Add new claim + Add a group claim Columns | Got feedback?

Required claim

Claim name	Value
Unique User Identifier (Name ID)	user.userprincipalname [nameid-format:emailAddre... ***

Additional claims

Claim name	Value
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emaila...	user.mail ***
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenn...	user.givenname ***
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	user.userprincipalname ***
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surna...	user.surname ***
<b>Rom_Azure_Groups</b>	<b>user.groups</b> ***

Advanced settings (Preview)

ISE Side نم ةشاش ةطوقل

Cisco ISE Administration

Identities Groups **External Identity Sources** Identity Source Sequences Settings

External Identity Sources

- Certificate Authentication F
- Active Directory
- LDAP
- ODBC
- RADIUS Token

Identity Provider List > [Redacted]

**SAML Identity Provider**

General Identity Provider Config. Service Provider Info. **Groups**

**Groups**

Group Membership Attribute Rom\_Azure\_Groups

+ Add Edit Delete

### (لوصول اضفر مت) SAML ةباجتس | ف ةددت مت تاومجم 1b ةلكشملا

دق نوكت نأ بجي ف، ةلجالا يه هذه تناك اذا. ةدحاو ةومجم نم رثكأ في اوضع سيل مدختس ملنا نأ نم دكأت ف، ةلكشملا قباسلا جالصالا لحي مل اذا مت. SAML ةباجتسا نم ةمئاقلا في طرف (فرعم / ةومجملا مسا) لوالا ةمئاقلا ISE قباطت ثيح [Cisco CSCwa17470](https://www.cisco.com/c/en/us/techdocs/cscwa17470.html) نم اءاطالا حيحصت فرعم تهجاو 3.1 P3 في اءطالا اذه لحي

جانب لوخدلا ليجست نكمي تحت iAdmins ةومجملا ISE نييعت نيوكت بجي، اقباسم اهميدقت مت يتلا IdP ةباجتسال اقفو

Cisco ISE Administration · Ident

Identities Groups **External Identity Sources** Identity Source Sequences Settings

External Identity Sources

- Certificate Authentication F
- Active Directory
- LDAP
- ODBC
- RADIUS Token
- RSA SecurID
- SAML Id Providers

Identity Provider List > [Redacted]

**SAML Identity Provider**

General Identity Provider Config. Service Provider Info. **Groups** Attrib

**Groups**

Group Membership Attribute Rom\_Azure\_Groups

+ Add Edit Delete

<input type="checkbox"/>	Name in Assertion	Name in ISE
<input type="checkbox"/>	iseadmins	Super Admin

### 404 دروم يلع روثعلا متي مل: 2 ةلكشملا

## [ 404 ] Resource Not Found

The resource requested cannot be found.

في أخط رهطي **guest.log**

```
2021-10-21 13:38:49,308 ERROR [https-jsse-nio-10.200.50.44-8443-exec-3][[]
```

```
cpm.guestaccess.flowmanager.step.StepExecutor -:-
```

```
Can not find the matched transition step on Step=id: 51d3f147-5261-4eb7-a1c9-ce47ec8ec093,  
tranEnum=PROCEED_SSO.
```

### لحل/البسلا

طقق لوالا فرعما نزم عاشنا دعب ةلكشملا هذه ةطخالما مت

ببترتال سفن بيلاتال برج، ةلكشملا هذه لحل:

(دعب لبالا فرعما ةلازاب مقن ال) ISE في ديدج SAML فرعما عاشناب مق 1. ةوطخال

اذه ديدجال IdP لى لوؤسما لوصو نبييعت ب مقو لوؤسما لى لوصول ةحفص لى لقتنا 2. ةوطخال

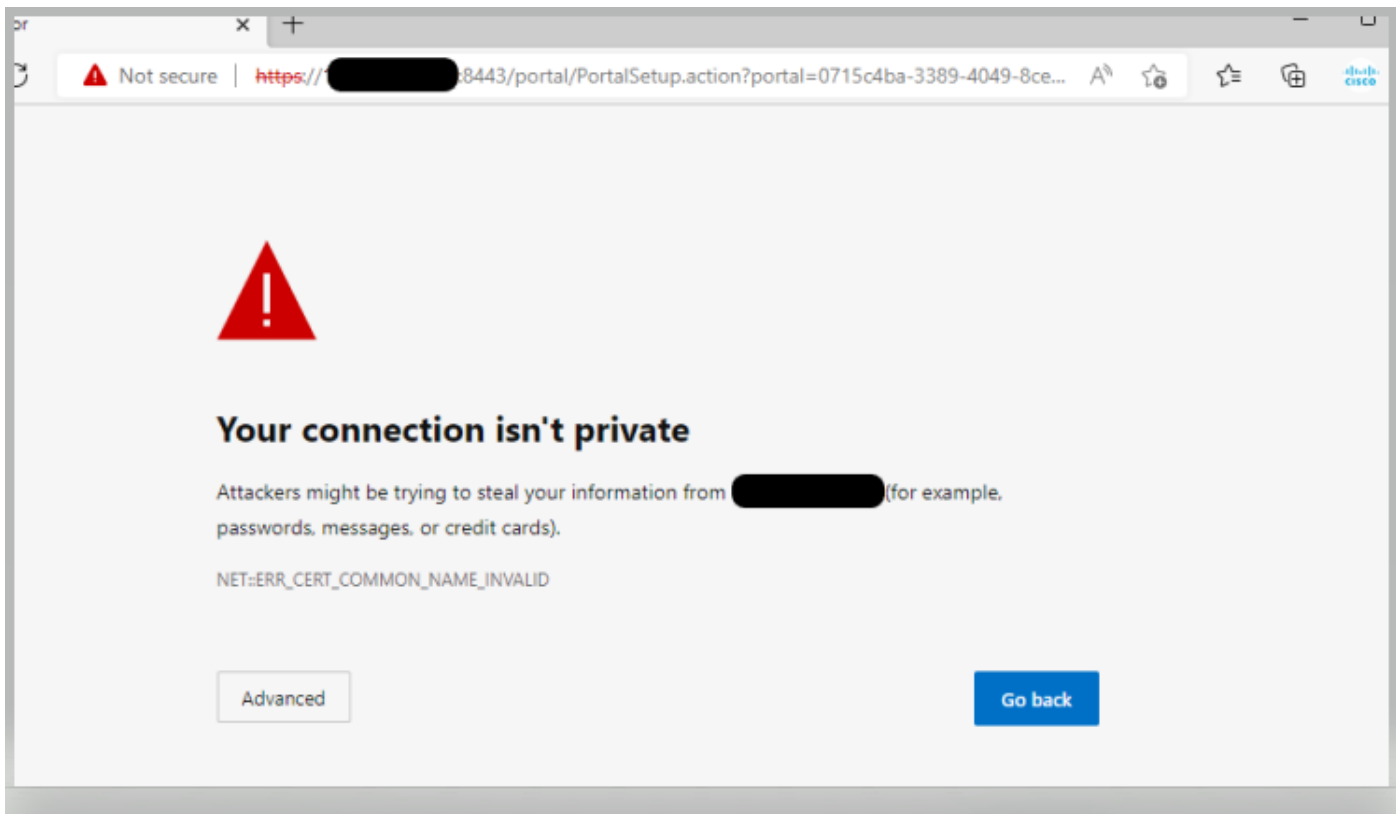
ةجراخال ةيوهلا يرفوم ةحفص في مبدقلا فرعما فذجا 3. ةوطخال

ةومجملل ةيرورض تانيييعت يا اراجاب مقو 1 ةوطخال في هؤاشنا مت ديدج فرعما لى لبالا IdP فيرعت تانايا داريتساب مق 4. ةوطخال

لك لذججنيسو، SAML لى لوخدلا ليجست لوا نألا 5. ةوطخال

### ةداهشلا ريذحت 3: ةلكشملا

ضرعتسما في اهب قوؤوملا ريغ ةداهشلا ريذحت ىرت نأ كنكمي، "SAML مادختساب لوخدلا ليجست" لى رقتن امدنع، دقعلا ددعت مشنلا في



## لحل/الاب س ل

نكي مل اذا، PKI رشن ضعب يف عدهاشلا ريذحت ىل ايدؤي اذهو. FQDN س يلو، IP طاشنن ال PSNs ىل اكهيجوت عداع اب pPAN موقت، اتالاحل ا ضعب يف SAN ل قح يف IP ناوئع كانه.

صخيخرتل نم لاجم SAN ل يف ip فيضي نأ workaround ل.

3.1p1 يف اذه لحت. Cisco [CSCvz89415](https://www.cisco.com/c/en-us/technical/tips/3.1p1.html) نم عاطخال احيحصت فرعم

ةمچرتل هذه لوج

ةللأل تاي نقتل نم ةومچم مادختساب دن تسمل اذہ Cisco تچرت  
ملاعلاء انءمچي فني مدختسمل معدى وتحم مي دقتل ةيرشبل او  
امك ةقيقد نوك تنل ةللأل ةمچرت لصف أن ةظحال مچري. ةصاخل مهتبل ب  
Cisco يلخت. فرتحم مچرت مامدقي يتل ةيفارتحال ةمچرتل عم لالحل وه  
ىل إأمئاد ةوچرلاب ي صؤت وتامچرتل هذه ةقد نع اهتيل وئسم Cisco  
Systems (رفوتم طبارل) ي لصلأل يزي لچن إل دن تسمل