

# هنيوكتو Shibboleth (IDp) ةيوه رفوم تيبتت SSO نيكمتل Cisco (IDs) فيرعت ةمدخل

## تايوتحمل

[ةمدقمل](#)

[ةيساسأل تابلطتمل](#)

[تابلطتمل](#)

[ةمدختسمل تانوكمل](#)

[تيبتت](#)

[ماظنل تابلطتمل](#)

[نيوكتل](#)

[LDAP مداخل عم لمكتل](#)

[نيوكتل فلم جذومن](#)

[عالمعل عيمج نم تابلطلاب حامسمل](#)

[تافرعمل عم لمكتل Shibboleth نيوكت](#)

[تافرعمل في فيرشتل نيوكتو \(SHA1\) ةنمأل ةئزجتل ةيمزراوخ](#)

[SAML ةباجتسلى لى user PRINCIPAL و UID نيوكت](#)

[IDp فيرعت تانايب](#)

[فيرعتل تانايب فيرفوم نيوكت](#)

[SSO ل نيوكتل نم ديزم](#)

## ةمدقمل

ليجست نيكمتل OpenAM (IDp) ةيوه رفوم لىل دوجومل نيوكتل دنسمل اذه فصى  
(SSO) يداخل لودل.

### Cisco تافرعم رشن جذامن

رشنل جتنمل

UCCX كراشم ميقم

PCCE (ةرشابم تانايب) LD و (Cisco Unified Intelligence Center) CUIC عم كرتشم ميقم

UCCE 2k رشن تايلمعل LD و CUIC عم ميقم كراشم

ةيلمعل فلأ 12 و فالأ 4 غلبت يتل رشنل تايلمعل ةلقتسم.

## ةيساسأل تابلطتمل

### تابلطتمل

ةيلال عيضاوملاب ةفرعم كيذل نوكت نأ Cisco يصوصت:

- Cisco Unified Contact Center Express (UCCX) رادصل 11.6 وأ Cisco Unified Contact Center Enterprise رادصل 11.6 وأ Packaged Contact Center Enterprise (PCCE) رادصل 11.6 بسخ  
ءاضتقالا.



	تانايب/ \${idp.home} في دامتعال ريغتم وه idp.home نإ شح هنا إلى عهريصت متي يئي ب java_opts في setenv.sh حيتافم نزم ليحتل دروم طبر طاقن إلى عوتحي Java	٪{idp.home}/credentials/ldap-server.trus
idp.authn.ldap.trustStore	في فليحم فلم ةءاع، ةقث دامتعال تانايب/ ٪{idp.home} LDAPAttributes ةمئاق يتل ةلصافب ةمسقملا عاجرا تدرا إذا. اهعاجرا مزلي	*
idp.authn.ldap.returnAttributes	BaseDN يتل مزلي عارج LDAP اهدنع	CN=نامدختسملا، DC=Cisco، DC=com
idp.authn.ldap.baseDN	شحبلا ديتر تنك إذا ام رركتم لكش ب	حيحص
idp.authn.ldap.subtreeSearch	LDAP ل شحبلا ةيفصت لمراع عارج دنع هب طبرلل DN شحبلا	(sAMAccountName={user})* administrator@cisco.com
idp.authn.ldap.userFilter	دنع اه ب طبرلل رورملا ةمك شحبلا عارج	
idp.authn.ldap.bindDN	ءاشنال قيسنت ةلسلس ةقءاصملا مدختسملا ل DNس لمعلا ريس في مكحتي شوح ةيفي ةفرعمل LDAP لباقم ةقءاصملا	٪s@adfserver.cisco.com (٪s@domainname) BindSearchAuthenticator
idp.authn.ldap.bindDNCredential	LDAP ليلدل لاصتال URI	

إلى عجرا، ليصافتلا نم ديزمل:

<https://wiki.shibboleth.net/confluence/display/IDP30/LDAPAuthnConfiguration>

## نيوكتال فلم جذوم

```
#
#idp.authn.LDAP.responseTimeout = PT3S
## SSL jvmTrust certificateTrust
keyStoreTrust
#idp.authn.LDAP.sslConfig = certificateTrust
## CertificateTrust
idp.authn.ldap.trustCertificates =
{idp.home}/credentials/ldap-server.crt
## keyStoreTrust TrustStore
idp.authn.ldap.trustStore =
{idp.home}/credentials/ldap-server.truststore
##
#idp.authn.LDAP.ReturnAttributes =
userPrincipalName sAMAccountName
idp.authn.ldap.returnAttributes = *
## DN ##
# DN anonSearchAuthenticator
bindSearchAuthenticator
# AD: CN=UsersDC=exampleDC=org
idp.authn.ldap.baseDN =
CN=usersDC=ciscoDC=com
idp.authn.ldap.subtreeSearch =
*idp.authn.ldap.userFilter =
(sAMAccountName={user})*
#
# AD:
idp.authn.ldap.bindDN=adminuser@domain.com
idp.authn.ldap.bindDN = @cisco.com
idp.authn.ldap.bindDNCredential = Cisco@123
```

```

# DN DirectAuthenticator
adAuthenticator
# AD idp.authn.ldap.dnFormat=s@domain.com
#idp.authn.LDAP.dnFormat =
s@adfssserver.cisco.com
# LDAP attribute-resolver.xml
# V2
idp.attribute.resolver.ldap.ldapURL =
{idp.authn.ldap.ldapURL}
idp.attribute.resolver.ldap.connectTimeout =
{idp.authn.ldap.connectTimeout:PT3S}
idp.attribute.resolver.ldap.responseTimeout =
{idp.authn.ldap.responseTimeout:PT3S}
idp.attribute.resolver.ldap.baseDN =
{idp.authn.ldap.baseDN:undefined}
idp.attribute.resolver.ldap.bindDN =
{idp.authn.ldap.bindDN:undefined}
idp.attribute.resolver.ldap.bindDNCredential
= {idp.authn.ldap.bindDNCredential:undefined}
idp.attribute.resolver.ldap.useStartTLS =
{idp.authn.ldap.useStartTLS:}
idp.attribute.resolver.ldap.trustCertificates
=
{idp.authn.ldap.trustCertificates:undefined}
idp.attribute.resolver.ldap.searchFilter =
(SAMAccountName=$resolutionContext.principal)

```

## ءالمعلا عيمج نم تاب لطلاب حامسلا

لىع تاريخي غت لاخدا مزلي، ءالمعلا عيمج نم ءدراولا تاب لطلال لوصو نامضلو  
"\$shibboleth\_home/conf/access-control.xml"

```

<entry key="AccessByIPAddress">
<bean id="AccessByIPAddress" parent="shibboleth.IPRangeAccessControl"
p:allowedRange="#{ {'127.0.0.1/32','0.0.0.0/0', ':1/128', '10.78.93.103/32'} }" />
</entry>

```

IP قاطن أ نم تاب لطلاب حمسي اذهو. اهب حومسملا تاقاطنلا لىل '0.0.0.0/0' فضا

## تافرعمل عم لمالك تلل Shibboleth نيوكت

تافرعمل ي ف ريفش تال نيوكتو (SHA1) ءنم آلا ءئزجتلا ءيمزراوخ

"\$shibboleth\_home/conf/idp.properties" حتفا، SHA1 لىل يضارتفا لكشب تافرعمل نيوكتل  
طبضاو:

```
idp.signature.config = shibboleth.SignatureConfiguration.SHA1
```

تريغ تنك اضيأ عي طتسي ليكشت اذه:

```
IDP.Encryption.إيرايختخ = true
```

ءم ادختسال ريفش حتاتفم عقوم ديدحت ي ف لشفلا يدؤي نلف، true لىل ءن يي عتبت تمق اذا،  
ريفش تلل ي، "يزاهتنا لكشب" ريفش تال ءارج احي تي اذه. ب لطلال لشف لىل، ءن ي كمت دنع  
(هب ريفش تلل ريطانللا في رعت تانا ي ب ي ف قفاوتم حتاتفم لىل ع روثعلا متي) نكم املك  
ىرخا ءقيرطب ريفش تال ي طختل نكلو.

## SAML ءباجتس لىل user\_PRINCIPAL و UID نيوكت

نيي عتل "\$shibboleth\_home/conf/attribute-resolver.xml" ي AttributeDefinition ءفاضا متت

SAML. ةباحتسإ ي ف user\_principal و فرعملإ ىلإ userPrincipalName و sAMAccountName

<DataConnector> ةمالمال ةمدختساب ldap ل صوم تادادعإ فضا، كلذىلإ ةفاضلإاب

ةظالم "userPrincipalName sAMAccountName ةمىقلااب ReturnAttributes دىدحت مزلي: ةظالم

Active Directory (AD) عم لماتك دوجو ةلاح ي ف ةيمازلل LDAPPProperty دعت: ةظالم

"\$shibboleth\_home/conf/attribute-filter.xml" ي ف تاريغيغتلا جمد

نيمضتلل \$shibboleth\_home/conf/saml-nameid.xml ريغيغت

## IDp فيرعت تانايب

idp- metadata.xml فلم لىمحت نكمي . "\$shibboleth\_home/metadata" دلجملا ي ف IDp فيرعت تانايب رفوتت (API) تاقىبطلتلة جمر ب ةهجاو لال خ نم تافرعمللا ىلإ idp-metadata.xml

عضو https://<idshost>:<idsport>/ids/v1/config/idpmetadata

"8553" يه ةمىقلاو نىوكتلل الباق انايك تسيل IDSPORT شىح

عيقوت ةداهش و، عيقوت ي تدهاش ىلع Shibboleth فيرعت تانايب يوتحت نأ نكمي: ريذحت idp-backchannel.crt in فلملا ىلإ لقتنا. ةيفللخال ةانقلاو ةملاع ةداهش تناك اذا. ةيفللخال ةانقلا ةداهش ىلع فرعتلل "\$shibboleth\_home/credentials" ةيفللخال ةانقلا ةداهش ةلازا كىلع بجي، ةىلوالا تانايبلا ي ف ةحاتم ةيفللخال ةانقلا Fedlet 12.0 ةبتكم نأل كلذو. تافرعمللا ىلإ لىمحتلا لبق xml فيرعتلا تانايب نم ةلاح ي ف. فيرعتلا تانايب ي ف طوق ةدحاو ةداهش معدت تافرعمللا اهمدختست ي تلال ةحاتم ةداهش لواحاتفملا مدختسي، ةدحاو عيقوت ةداهش نم رثكأ رفوت

فيرعتلا تانايب يرفوم نىوكت

في لاداء عم فيرعتل تانايب يرفوم نيوكت لاداءاتحن  
providers.xml.

```
<MetadataProvider id="smart-86" xsi:type="FilesystemMetadataProvider"  
metadataFile="/opt/shibboleth-idp/SP/sp.xml"/>
```

ديرف مسا يا "id" ةمس نوكت نا نكمي ثيح

فيرعتل تانايب ناو ددحمل لافرم لاب لجم فيرعتل تانايب رفوم نا لاداءل اذهريري شي  
/opt/shibboleth-idp/SP/sp.xml ددحمل لاداءل في ةرفوم

في ددحمل MetadataFile لاداءل تافرم لاب ةصاخلا (SP) ةمدخل رفوم فيرعتل تانايب خسن بجي  
لاداءل.

GET ربع تافرم لاب ةصاخلا SP فيرعتل تانايب دادرتسا نكمي: ةظحالم  
الباق انايك تسيلا IDsport، <https://<idshost>:<idSport>/ids/v1/config/spmetadata>،  
"8553" هه ةمقلاو نيوكتلل

## SSO ل نيوكتلل نم ديزم

نم ديزم ل. ةمدخ ةيوه cisco عم لم اكني نا SSO ل بناج idP ل نم ليكشلتل ةقويثو اذهرصي  
ي: درفلال جتنم ل نيوكتلل لاداءل عجرا، لاداءل

- [UCCX](#)
- [UCCE](#)
- [PCCE](#)

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 ةل فارتحال ةمچرتل عم لاعلاء و  
ىل إأمءءاد ءوچرلاب ةصوء و تامةرتل هذه ةقء نء اهءل وئس م Cisco  
Systems (رفوتم طبارل) ةل صأل ةل ءل ءن إل دن تسمل