

ةرادال ةيچراخال SAML SSO ةقداصم نيوكت ESA و SMA

تايوتحمل

[ةمدقمل](#)

[ةيبل](#)

[ةيساسال تابلطتمل](#)

[نيوكتلالبوقامرايتخل ةمئاق](#)

[ةيساسا تامولعم](#)

[ةمدخ دوزمك ESA/SMA نيوكت](#)

[ESA/SMA ةزهجأ عم لمعلل \(IDP\) ةيوهلا رفوم نيوكت مرق](#)

[ESA/SMA ىلع ايلخاد نيديرشمل تادادعلا نيوكت](#)

[ESA/SMA ىلع SAML مادختساب ةيچراخال ةقداصم نيوكت](#)

[امجالص او عاخال افاشكتسا](#)

[لوخدلا ليچست مادختسا \("\) لوخدلا ليچست ةحفص ي ف SSO هيوت ةداعلا طابترا رهظي ال
\("\) يدخال](#)

[ةقداصم لشف عم ESA/SMA ىل لوخدلا ليچست ةحفص ىللا هيوتل ةداعلا ةيلمع عجرت
لوؤس ملاب لاصتالا اعزل! يدخال لوخدلا ليچست](#)

[اعزل! اضيوفتل لشف عم ESA/SMA ىل لوخدلا ليچست ةحفص ىللا Redirect عجرت
لوؤس ملاب لاصتالا](#)

[ةلص تاذا تامولعم](#)

ةمدقمل

و ESA ماظن ةرادال SAML 2.0 SSO ل ةيچراخال ةقداصم نيوكت ةيفيكن دننتملا اذه حضوي
SMA.

ةيبل

- (SMA) نامال ةرادا ةزهجأو (ESA) نيورتكلال دبرل ناما ةزهجأ: تاجت نمل
- SMA و ESA ماظن ةرادا: ىلع قبطني
- ىوتسم ىلع IdP و (SP) ةمدخال رفوم تافيصوت نيوكت متي: ةومجمل ماظن كولس
ةومجمل ماظن ىوتسم ىلع ةيچراخال ةقداصم نيوكت متي؛ زاهجلا

ةيساسال تابلطتمل

- ESA/SMA بيولا ةهجاو ىل يرادال لوصول

- وأيضاً عيقت (PEM) وأ (PKCS #12 (PFX) قيسنتب نحاتم صاخلا حاتفملاو X.509 ةداهش (CA) عيقت
- تانايبب صاخلا URL ناوعو ةيجراخ ةهجب صاخلا (IdP) ةيوهلا رفوم قيبطت ىلا لوصولا هب صاخلا SSO/فيرتلا

نيوكتلا لبق ام رايتخا ةمئاق

- لوصولل نولوؤسملا اهمدختسي يتلا ةرادلا ةهجاول FQDN/فيضملا مسا نم ققحتلا مسا عم ديكأتلا (ACS) كلهتسملا ةمدخل URL ناوع قباطت ديكأت؛ زاهجلا ىلا فيضملا
- زاهجلا ىوتسم ىلا SAML نيوكتلا طيختلاب مقف، ةعومجم ماظن في زاهجلا ناك اذا ةيجراخلا SAML ةقداصم نيكتمت لبق وضع لكل
- زاهج لكل لصفنم قاطن وأ قيبطت بلطتلا IdP ناك اذا ام ددح
- ةبولطملا حيتافملاو تاداهشلا رفوت نم دكأت
- ESA/SMA رود نييعتلا ةبولطملا رودلا وأ ةعومجملا ةمس لسري IdP ديكأت

يئاهنلا مدختسملا لزعب صاخلا SAML SSO ىلا دنتسملا اذه قبطني ال: ريذحت (EUQ).


ةيساساً تامولعم

- جذومن ريفوت متي. ةيجراخلا ةهجلل IdP نيوكتلا ينقتلا معدلا Cisco TAC رفوي ال ةعئاشلا IdPs تافرتمل نيوكتلا عجارمل


SSO SAML IDps

- تامدخ عم ةلماك، لماعلا ةيئانث ةقداصم (DAG) ةيئانثلا لوصولا ةرابع فيضت SAML 2.0 داحتا مادختساب ةعئاشلا ةباحسلا
- Azure و 3 و 2 و ADFS مادختساب اهرايتخا مت - Active Directory (ADFS) ةمدخ داحتا تامدخ PingFederate و SecureAUTH و Active Directory (Azure AD)
- لمع راطلا لخاد اهمعدي IdP ناك اذا ةيفاضا لم اوعلا ةيئانث ةقداصم مادختسا نكمي SAML 2.0 يداحالا لوخدلا ليحست
- ةمدخل معددي يذلا IdP مادختساب ةقداصملا OKTA معددي

ةمدخ دوزمك ESA/SMA نيوكت

 عيمجل زاهجلا يوتسم لىلا نيوكتلا ةعومجم ماظن ي ةدوجوملا ESAs بلطتت :ةظحالم SAML نيكمت لبق ةعومجملا ماظن اعاضأ

- ةزهجال ربع نيوكتلا اذه ةكراشم ،ةحفصلا لفسأ ي ةدوجوملا رايلخلا ديدحت ةلاح ي طورشلا هذه قيبطت متي ،ةعومجملا ي ةدوجوملا
- كلهتسملا URL اناثتساب ةعومجملا ماظن اعاضأ لىلا لوقحلا ةفاك خسن متي ديكأتلا
- صاخلا فيضملا مسا ميمعتب ديكأتلا كلهتسملا صاخلا URL ناووع موقى ACS. اهنأ لىلا ايئاقلا ةرادلا ةهجاوب
- فيضملا لىلا لوصولل ليدب فيضم مسا مدختست يتلا تائيبل بلطتت CES. ةفاضتسملا ةزهجالا ،لاثملا لىلا سىلا ،فيضم لكلا يوديلا نيوكتلا
- SMA و ESA ةهجاوب ي SP ليثم ةيمستل مدختسملا مسالا :فيرعتلا فلم مسا
- ةيمستلا وه مسالا اذه IdP. هاري امك SP ليثمل مدختسملا مسالا :نايكل فرعم لىلا سىلا ،مسا ي اذه نوكتي نا نكمي . SP ليثمتل فرعملا اهمدختسي يتلا ESA_SSO و ESA_SP ،لاثملا
- نيوكتلا لىلا ريق لوقح :مسالا فرعم قيسنت
- IdP لبق نم مدختسملا URL ناووع :ACS) االمعلا ةمدخ و كلهتسملا URL ديكأت اذه ESA/SMA فيضم لاصتالا
- SP ةداهش
- PEM و PFX/PKCS12 قيسنتب ةصاخ/ةماع X.509 تاداهش :قيسنتلا
- اهؤاشنإ مت يتلا تاداهشلا نم ددح :تاداهشلا ةمئاق نم ديدحت :1 رايلخلا تاداهشلا > ةكبشلا نمض ESA لىلا لعفلاب
- PEM قيسنتب حاتفمو ةداهش ليحت :حاتفملاو ةداهشلا ليحت :2 رايلخلا
- PKCS #12 فلم ليحت :PKCS #12 تاقاطب ليحتب مق :3 رايلخلا
- يداحأ لوخد ليحتسلا ESA/SMA لىلا ايتاذ ةعقوم ةداهش اشنا :يرايلخا SAML.
- ابولطم كلذ ناك اذا رورم ةمكب صاخلا حاتفملا ةيماحب مق

 ي صاخ حاتفمو صيخرت لك ظفحا ، PEM قيسنتب تاداهش مادختسا مت اذا :ةظحالم ةلصفنم تافللم

SAML Settings

Service Provider Settings

Profile Name: [REDACTED]_SSO

Configuration Settings:

Entity ID: [REDACTED]

Name ID Format: urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified

Assertion Consumer URL: https://dh[REDACTED]-esa2.example.com

SP Certificate:

Select from Certificate List: [Select a Certificate... ▼]

Upload Certificate and Key: [?]

Upload PKCS #12: [?]

Uploaded Certificate Details:

Issuer: C=US\CN=SAML_SSO\L=Raleigh\O=Cisco\ST=NC\EmailAddress=[REDACTED]\OU=ESA_TAC

Subject: C=US\CN=SAML_SSO\L=Raleigh\O=Cisco\ST=NC\EmailAddress=[REDACTED]\OU=ESA_TAC

Expiry Date: Sep 21 16:16:12 2022 GMT

Sign Requests

Sign Assertions

Make sure that you configure the same settings on your Identity Provider as well.

Organization Details:

Name: chris corp

Display Name: Chris

URL: https://cisco.com

Technical Contact:

Email: [REDACTED]

Share this configuration across machines in cluster [?]

Duplicates all settings except the Assertion Consumer URL

ةمدخلال رفوم دادع| ةحفص

ةمدخلال رفوم دادع| ةحفص

- IdP إلى لسررم ال ESA/SMA SAML لاصتا عي قوت را يخ : تا بل لطلال عي قوت
- ESA/SMA إلى ةلسررم ال تا دي كأتال عي قوت IdP نم بل طي را يخ : تا دي كأتال عي قوت
- ةبسانم ال ةك رشال تا نا يا بب اهتئبعت نكمي : ةسسؤم ال لي صافات
- تا دادع ال إلى ع ظا فحلل اه ذي فنن و تا ري يغتال لاسرا
- SAML ني وكت ةحفص نم SP في رعت تا نا يا بب لي زنن تب مق

ESA/SMA ةزهجأ عم لمعلل (IdP) ةي وهال رفوم ني وكت تب مق



علع) ESA. لك لة لصفنم تا لاماعم وأ تا قي بطت تا فرعم ال ضع ب بل طتت : ةظحال م
DUO: تا ثم ال لي بس

رشنللا تقويف ةددعتم تافرعم تانيوكتل اجذومن تااطابتراللا هذه رفوت
عجارمك ةلثمألا هذه رفوت متي . ثلثاللا فرطاللا تاجت نمل ينفاللا معدللا Cisco TAC رفوي ال

ESA/SMA ىلع ايلخاد ني درشملا تادادع ا نيوكت

1. SAML > ماطنللا ةرادا ىللا لقتنا .

2. ةيوفه رفوم ةفاضلا ددح .

- نإحاتم نارايخ كانه
- IDp فيرعت تانايب داريتس
- ايودي حيتافملا نيوكت
- IdP فيرعتل مدختست ةميق يأ نوكت نأ نكمي : نايكللا فرعم
- SAML ةقادصم تابلط SP هيللا لسري يذاللا SSO: URL تامولعم عقوم ددحم
- ةلصفنم تافلم يف ةماعلا ةداهشلاو صاخلال حاتفملا ليحت

3. تادحو ةفاك ربع نيوكتللا خس نل ةعومجملا يف ةدوجوملا ةزهجالا ربع نيوكتللا اذه ةكراشم .
ةعومجملا يف ESA

SAML Settings

Identity Provider Setting

Profile Name:

Configuration Settings: Configure Keys Manually

Entity ID:

SSO URL:

Certificate: No file selected.

Uploaded Certificate Details:

Issuer: C=US\CN=SAML_SSO\L=Raleigh\O=Cisco\ST=NC
\emailAddress=... \OU=ESA_TAC

Subject: C=US\CN=SAML_SSO\L=Raleigh\O=Cisco\ST=NC
\emailAddress=... \OU=ESA_TAC

Expiry Date: Sep 21 16:16:12 2022 GMT

Import IDP Metadata No file selected.

Share this configuration across machines in cluster

ايودي IDp ىوتحم لاخدا

ايودي IDp ىوتحم لاخدا

4. IDP نم فيرعتل تانايب لي محت

- IDP فيرعت تانايب داريتس ا دح
- نيوكتل ظفح او IdP نم ظوفح مل فيرعتل تانايب فلم ىل ا حفصت
- ىل ق بطني ناك اذا عومجم في ةزهجالا ربع نيوكتل اذه ةكراشم رايل ر فوتي رشنل

SAML Settings

Identity Provider Setting

Profile Name: AZURE_IDP

Configuration Settings:

Configure Keys Manually

Entity ID: [Redacted]

SSO URL: [Redacted]

Certificate: [Browse... No file selected.]

Import IDP Metadata

[Browse... No file selected.]

Uploaded Metadata Details:

Entity ID: https://sts.windows.net/ea6064aa-28e1f39e0b/

SSO URL: https://login.microsoftonline.com/ea6064aa-28e1f39e0b/saml2

Share this configuration across machines in cluster ? **Duplicates all settings to Cluster Members**

نيحزانل نم فيرعتل تانايب لي محت

نيحزانل نم فيرعتل تانايب لي محت

ESA/SMA ىل ع SAML مادختساب ةي جراخل ةق داصم ل ني كمت

نيي عتل نيي عت SAML ي داخال لوخدل لي جست بلطتي، ةي جراخل LDAP ةق داصم لثم ةي رادل راودال تاعومجم

1. > ةي جراخل ةق داصم ل > (عومجم لى وتسم) نوم دختسم ل > ماظنل ةرادا ىل لقتنا 1. ني كمتل

2. لماس: ةق داصم ل عون دح.

3. نيي عت نم شحلل ةمس ل لسا ل خدأ: (ي رايخا) مسالا ةطيرخ ةق باطل ةمس ل لسا 3. ةعومجم ل

ليحرتل لايوهال رفومل اهنويوكت مت يتل تامسلا لىل ع م س ل ا م س ا د م ت ع ي : ع ظ ح ا ل م
ي ف د د ح م ل ا م س ل ا م س ا ل ع ق ب ا ط م ل ا ت ا ل ا خ د ا ل ا ن ع ز ا ه ج ل ا ش ح ب ي . S A M L ع ب ا ج ت س ا ي ف
ن ي و ك ت م ت ي م ل ا ذ ا . ع و م ج م ل ا ن ي ي ع ت ل ق ح ي ف ع ن و ك م ل ا ت ا م س ل ا ل ب ا ق م S A M L ع ب ا ج ت س ا
ل ب ا ق م S A M L ع ب ا ج ت س ا ي ف ع د و ج و م ل ا ت ا م س ل ا ع ف ا ك ن ع ش ح ب ل ا ب ز a ه ج ل ا م و ق ي ، ل ق ح ل ا ا ذ ه
ا ه ن ي و ك ت م ت ي ت ل ا ع و م ج م ل ا ن ي ي ع ت ل ق ح

د د ح م ل ا م د خ ت س م ل ا ر و د ل ا ا د ا ن ت س ا S A M L ل ي ل د ي ف ع ف ر ع م ي ه ا م ك ع و م ج م ل ا م س ا ع م س ل خ د ا . 4.
ص ص خ م ل ا و ا ق ب س م

- ت ا ع و م ج م ع م س ع ف ا ض ا ن ك م ي . ع و م ج م ع م س ل ع و م ج م ل ا ن ي ي ع ت ل ق ح ي و ت ح ي ن ا ب ح ي
ا ه ت ا ب ا ج ت س ا و S A M L ت ا د ي ك ا ت ع ق د ا ص م ل ع د د ح م ر ي غ

External Authentication Settings		
<input checked="" type="checkbox"/> Enable External Authentication		
Authentication Type:	SAML	
SAML Profile:	SAML profile has been configured at System Administration > SAML	
Attribute Name for Matching the Group Map: ?	memberOf <small>The Attribute Name, separate multiple entries with a comma</small>	
Group Mapping:	Group Name in Directory	Role ?
	ESA_Admins	Cloud Administrator
<small>Group names are case-sensitive.</small>		
<input type="button" value="Cancel"/>		<input type="button" value="Submit"/>

ةيخرال ع ق د ا ص م ل ا ت ا د ا ع ا

ةيخرال ع ق د ا ص م ل ا ت ا د ا ع ا

5. ا ه ذ ي ف ن ت و ت ا ر ي ي غ ت ل ل ا س ر ا .

ع ح ف ص ض ر ع ت . ل و خ د ل ا ل ي ج س ت ع ح ف ص ل ف س ا ي ف د ي د ج ط ا ب ت ر ا ض ر ع م ت ي ، ن ي و ك ت ل ا ح ا ج ن د ع ب
ه ي ج و ت د ي ع ي ي ذ ل ا ي د ا ح ا ل ا ل و خ د ل ا ل ي ج س ت م ا د خ ت س ا ط ا ب ت ر ا E S A / S M A ل ا ل و خ د ل ا ل ي ج س ت
(I D p) . ع ك ر ش ل ا ع ي و ه ر ف و م ل ا ن ي ل و و س م ل ا

ع ص ا خ ل ا S A M L ل ا ل و خ د ل ا ل ي ج س ت ع ح ف ص ل ا ل و و س م ل ا ه ي ج و ت ع د ا ع ا م ت ت ، ه د ي د ح ت د ن ع
ة ك ر ش ل ا ب



SAML ىل هه هيجوت ةداع| متيس يذلا يداحألا لوخدلا ليجست طابترا مادختسا

SAML ىل يداحألا لوخدلا ليجست طابترا هيجوت ةداع| تاي لمع مادختسا

اهحالص او عاطخألا فاشكتسا

IdP نيوكت وأ زاهجال نيوكتب ةقلعتم ةلكشملا تناك اذا ام ديدحتل تارشؤملا هذه مدختسا

مادختسا") لوخدلا ليجست ةحفص ي ف SSO هيجوت ةداع| طابترا رهظي ال
("يداحألا لوخدلا ليجست

SAML > ةيجراخالا ةقداصملا > نيمدختسملا > ماظنلا ةرادا نيوكت نم دكأت

لش ف عم ESA/SMA ىل لوخدلا ليجست ةحفص ىل هيجوتلا ةداع| ةي لمع عجرت
لوؤسملاب لاصتالا عاجرلا! يداحألا لوخدلا ليجست ةقداصم

لوؤسملاب لاصتالا عاجرلا! يداحألا لوخدلا ليجست ةقداصم تلشف": أطخالا

- IdP ي ف ةقداصملا تلشف
- ليجست ةقداصم ةحفص ىل لوصول ةطقن ىل لمعي نيوكتلا نأ ىل ريشي اذهو
دامتعالا تانايب لاسراو يداحألا لوخدلا
- IdP تاداع| نم يفاضل ققحت بلطتي و IdP نيوكت ىل لشفالا اذه عجري ام ابلاغ

!ضيوفتلا لش ف عم ESA/SMA ىل لوخدلا ليجست ةحفص ىل Redirect عجرت
لوؤسملاب لاصتالا عاجرلا

لوؤسملاب لاصتالا عاجرلا! ضيوفتلا لش ف": أطخالا

- ESA/SMA. يف ضيوفتلا لشف نكلو، ةقداصملا ريرمت مت
- SAML. > ةيجراخلا ةقداصملا > نيمدختسملا نمض تاداعالا ىلع زكر
- ةومجملا نييعتو، ةومجملا مسا، ةمسلا مسا

ةلص تاذا تامولعم

- [مدختسملا ةلدا - Cisco](#) نم ينورتكلاللا ديربلا نامأ ةزهجأ
- [مدختسملا ةلدا - Cisco](#) نم ىوتحملا نامأ ةرادا ةزهجأ
- [مدختسملا ةلدا - \(ببولا نامأ\) Cisco Web Security](#)

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