

# نمآ بي و زا ه ع م ة د د ع ت م ل ا ISE ت ا ع و م ج م ج م د TrustSec ل ا ة د ن ت س م ل ا ج ه ن ل ل

## ت ا ي و ت ح م ل ا

[ة م د ق م ل ا](#)

[ة ي س ا س ا ل ا ت ا ب ل ط ت م ل ا](#)

[ت ا ب ل ط ت م ل ا](#)

[ة م د خ ت س م ل ا ت ا ن و ك م ل ا](#)

[د و ي ق ل ا](#)

[ة ك ب ش ل ل ي ط ي ط خ ت ل ا م س ر ل ا](#)

[ن ي و ك ت ل ا](#)

[I S E ن ي و ك ت](#)

[S X P ن ي ك م ت](#)

[ة ع و م ج م ل ا م ا ط ن د ق ع ي ل ع S X P ن ي و ك ت](#)

[ع ي م ج ت ل ا ة د ق ع ي ل ع S X P ن ي و ك ت](#)

[ع ي م ج ت ل ا ة د ق ع ي ف p x G r i d ن ي ك م ت](#)

[p x G r i d ل ي ئ ا ق ل ل ت ل ا د ا م ت ع ا ل ا](#)

[ة ك ب ش ل ل ا ة ز ه ج ا ل T r u s t S e c ت ا د ا د ع ا](#)

[ة ك ب ش ل ل ا ز ا ه ج ض ي و ف ت](#)

[ب ي ق ر](#)

[ل ي و خ ت ل ا ة س ا ي س](#)

[\( ي ر ا ي ت خ ا \) I S E ع ي م ج ت ل ا ة د ق ع ي ل ع E R S ن ي ك م ت](#)

[\( ي ر ا ي ت خ ا \) E S R ة ر ا د ا ة ع و م ج م ي ل ا م د خ ت س م ة ف ا ض ا](#)

[ن م ا ل ا ب ي و ل ا ز ا ه ج ن ي و ك ت](#)

[p x G r i d ة د ا ه ش](#)

[ن م ا ل ا ب ي و ل ا ز ا ه ج ي ل ع E R S و S X P ن ي ك م ت](#)

[ف ي ر ع ت ل ا ف ي ر ع ت ف ل م](#)

[ب ي ق ر ل ا ي ل ع ة م ئ ا ق ل ل ا ز ي م ر ت ل ا ك ف ة س ا ي س](#)

[ل د ب م ل ا ن ي و ك ت](#)

[A A A](#)

[ك ي س و ر ت](#)

[ة ح ص ل ا ن م ق ق ح ت ل ا](#)

[ة ل ص ت ا ذ ت ا م و ل ع م](#)

## ة م د ق م ل ا

I S E ر ش ن ت ا ي ل م ع ن م ( S G T ) ن ا م ا ل ا ة ع و م ج م م ق ر ت ا م و ل ع م ل ا س ر ا ع ا ر ج ا د ن ت س م ل ا ا ذ ه ف ص ي ل ا ل خ ن م ( W S A ) ب ي و ل ا ن ا م ا ز ا ه ج م س ا ب ا ي م س ر ف و ر ع م ل ا ( C i s c o ) ن م د ح ا و ن م ا ب ي و ز ا ه ج ي ل ا ة د د ع ت م ل ا T r u s t S e c ر ش ن ي ف S G T ي ل ع ة م ئ ا ق ل ل ا ب ي و ل ا ي ل ل ا ل و ص و ل ا ت ا س ا ي س ن م ة د ا ف ت س ا ل ل P X g r i d .

ت ا س ا ي س ل I S E ن م ة د ح ا و ة ع و م ج م ع م ا ل ا ة ن م ا ل ا ب ي و ل ا ة ز ه ج ا ج م د ن ك م ي ا ل . 14.5 ر ا د ص ا ل ا ل ب ق ل ع ا ف ت ل ا ن م ا ل ا ب ي و ل ا ز ا ه ج ل ن ا ل ا ن ك م ي ، د ي د ج ل ر ا د ص ا ل ا ا ذ ه ل ا خ د ا ع م و . S G T ي ل ع ة م ئ ا ق ل ل ا ة ي و ه ل ا . ا ه ن ي ب ع م ج ت ي ت ل ا ة ل ص ف ن م ل ا I S E ة د ق ع م ا د خ ت س ا ب ة د د ع ت م ل ا I S E ت ا ع و م ج م ن م ت ا م و ل ع م ل ا ع م .

فلتخمنم نم مدختسملا تانايب ري دصتة ينيانكم انل حيتي ويري بك ةدئاف دوعي رمألا اذهو مدختسملل نكمي يتلا جورخلا ةطقن يف مكحتلا ةيحو (ISE) ةيوهلا تامدخ تاعومجم 1:1 جم دىل ةجالحا نود اهمادختسا

## ةيساسألا تابلطتملا

### تابلطتملا

ةيلالاتل عيضاوملاب ةفرعم كي دل نوكت نأ Cisco ي صوت

- (ISE) ةيوهلا تامدخ كرحم
- نمألا بيو زاهج
- RADIUS لوكوتورب
- كيسيورت
- pxGrid

### ةمدختسملا تانوكملا

ةيلالاتل ةيداملا تانوكملا او جماربلا تارادصا ىل دنننسملا اذه يف ةدراولا تامولعمل دننست

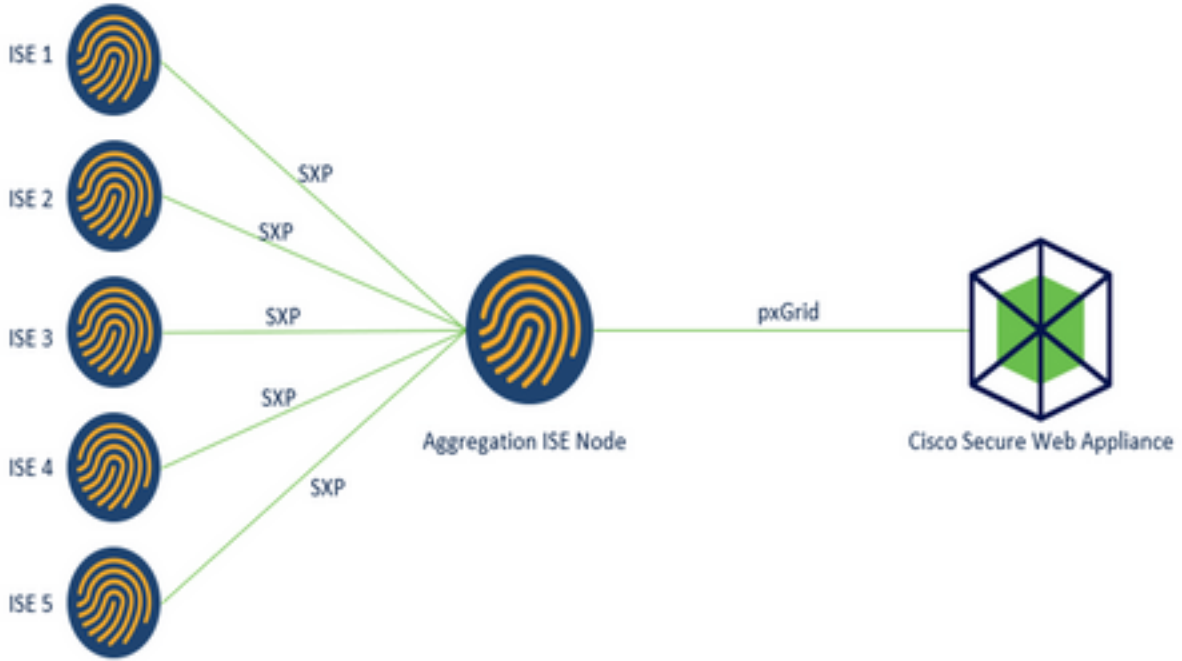
- 14.5 نمألا بيو زاهج
- 3.1 P3 رادصا ل ISE

ةصاخة يلمعم ةئيبي يف ةدوجوملا ةزهجالا نم دنننسملا اذه يف ةدراولا تامولعمل عاشننم مت تناك اذا. (يضايرتفا) حوسمم نيوكتب دنننسملا اذه يف ةمدختسملا ةزهجالا عيمج تادب رمألا لمحتملا ريثاتلل كمهف نم دكأتف، ليغشتلا ديقتك تكبش

### دويقلا

1. عابقرلل ةدوجوملا تانبيعتلا ىلع ظافحلا ىل ISE تاعومجم عيمج جاتحت.
2. ISE تاعومجم يقابب صاخلا SGTs مقر/مسا ISE عيمجت ةدقعل نوكي نأ بجي.
3. (هيحوتلا/ريغشتلا كفا/لوصولا) ةسايسلا ديحت ال نمألا بيو زاهجل نكمي ال مدختسملا مسا الو ةعومجملا ىل الو SGT ةمالع ىل ادانتسا
4. بيقرلا ىلع تامولعمل عبتتو ريراقتلا دادع دم تعي.
5. هذه ىلع اهقيبطت يف ةدوجوملا ISE/Secure Web Appliance مجح ديحت تاملعم رمتست. ةزيملا.

## ةكبشلل يطيختلا مسرلا



ةةلمعلا

1. تاسايس ىلا اءانتسا ابيقر ىقلى تي هن اء ؁ ءك بشلاب ىئاهنلا مءءتسملا لاصتا ءن ع . ISE فى لىوختلا
2. SGT تانىعت لكش فى هءه SGT تامولعم لاسراب لك ءءب ءفلءءملا ISE تاعومءم موقت . SXP لالء نم ISE عىمء ءءقعل IP
3. pxGrid ربع ءءاولا نم آلا بىولا زاى عم اهكراشتو تامولعمل هءه ISE عىمء ءءقعل ىقلى ت .
4. ءىناكم ارفوتل ىنفلال بىقرلا نم اهملعت ىتلا تامولعمل نم آلا بىولا زاى مءءتسى . بىولا ىلا لوصول تاسايس ىلا اءانتسا نىمءءتسملا ىلا لوصول

## نىوكءلا

### ISE نىوكء

#### SXP نىكمء

فى ءءوىرسىلا ءىولعل ءىوازلاب ءووم  ءءالءل رطسألا ءنوقى اءء . 1 ءوطءلا رشنلا > ماطنلا > ءءءلا

رىرء قوف رقناواهنىوكء ءىرء ىتلا ءءقعل ءء . 2 ءوطءلا

The screenshot shows the Cisco ISE Administration interface. The top navigation bar includes 'Deployment', 'Licensing', 'Certificates', 'Logging', 'Maintenance', 'Upgrade', 'Health Checks', 'Backup & Restore', 'Admin Access', and 'Settings'. The main content area is titled 'Deployment Nodes' and shows a table with one node: 'ise01-CL1'. The 'Edit' button for this node is highlighted with a red box. Other buttons like 'Register', 'Syncup', and 'Deregister' are also visible.

### SXP ةمدخ نيكمتم عبرملا ددح، SXP نيكمتم ل 3. ةوطخلا

The screenshot shows the 'Enable Session Services' configuration page in Cisco ISE. The 'Enable SXP Service' checkbox is checked and highlighted with a red box. Other services like 'Enable Profiling Service' and 'Enable Threat Centric NAC Service' are also visible but unchecked. The 'Use Interface' is set to 'GigabitEthernet 0'.

### ظفح قوف رقناو لفسألا لفسأل ريرمتم لاب مق 4. ةوطخلا

ةدقع نيكمتم متي شيح، ةومجم لك في ISE دقع يقابل تاوطخلا عيمج ررك: ةظحالم  
لا عيمجتلا.

### ةومجمملا ماظن دقع لىع SXP نيوكت

لىع ددحو ىرسىلا ةيولعل ةيوازلا في دوجوم  ةالثلا رطسألا ةنوقيأ ددح 1. ةوطخلا  
TrustSec > SXP > لمعلا زكرم.

SXP رىظنك ISE عيمجت ةدقع نيوكتل ةفاضلا قوف رقنا 2. ةوطخلا

The screenshot shows the 'SXP Devices' configuration page in Cisco ISE Work Centers. The '+ Add' button is highlighted with a red box. The page shows a table with 2 total rows and a 'Go' button. Other buttons like 'Refresh', 'Trash', 'Edit', and 'Assign SXP Domain' are also visible.

ددح. عمتمسم ك رىظنلا رود ددحو، ISE عيمجت ةدقع ل IP ناو نعومسالا فيرعتب مق 3. ةوطخلا

تحت نكمم ددحو، ةبولطملا SXP تالاجم، ةلصتملا PSN تاكبش تحت ةبولطملا PSN تاكبش  
بولطملا رادصلا او رورملا ةملك عون ددح م ث، ةلال

**Cisco ISE** Work Centers • TrustSec

Overview Components TrustSec Policy Policy Sets **SXP** ACI

**SXP Devices**  
All SXP Mappings

SXP Devices > SXP Connection

► Upload from a CSV file

▼ Add Single Device

Input fields marked with an asterisk (\*) are required.

Name  
ISE Aggregation node

IP Address \*  
10.50.50.125

Peer Role \*  
LISTENER

Connected PSNs \*  
ise01-CL1

Overview Components TrustSec Policy Policy Sets **SXP** ACI

**SXP Devices**

All SXP Mappings

SXP Domains \*  
default x

Status \*  
Enabled

Password Type \*  
CUSTOM

Password

Version \*  
V4

Advanced Settings

Cancel Save

## ظفح ةقطق ط. 4 ةوطخال

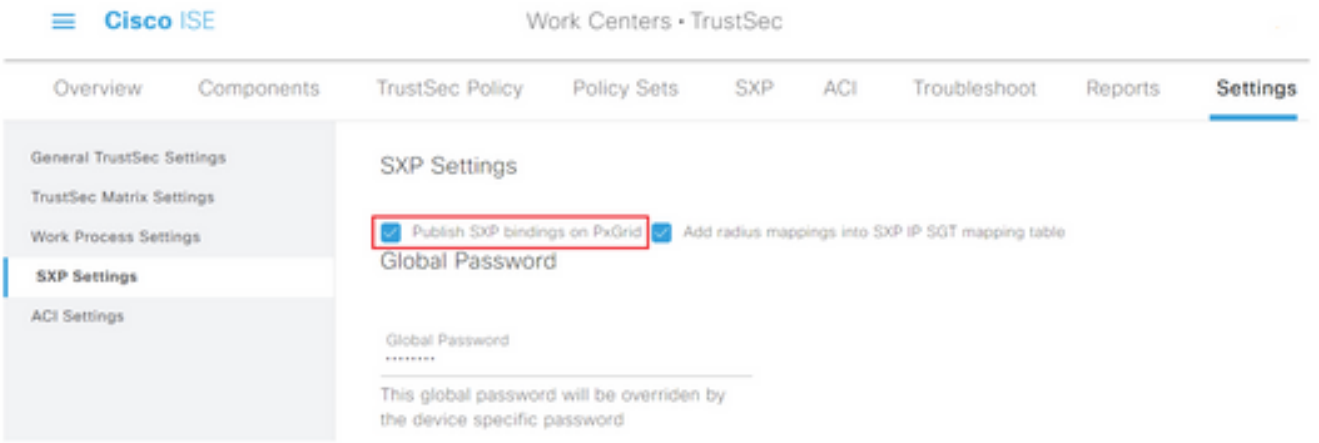
ةدقعب SXP لاصتا ءانبل ةعومجم لك في ISE دقع يقابل تاوطخال عيمج ررك: ةظحال م ريظن رودك توصول ربكم ددحو عيمجتلا ةدقع ىلع ةيلمعال سفن ررك. عيمجتلا

## عيمجتلا ةدقع ىلع SXP نيوكت

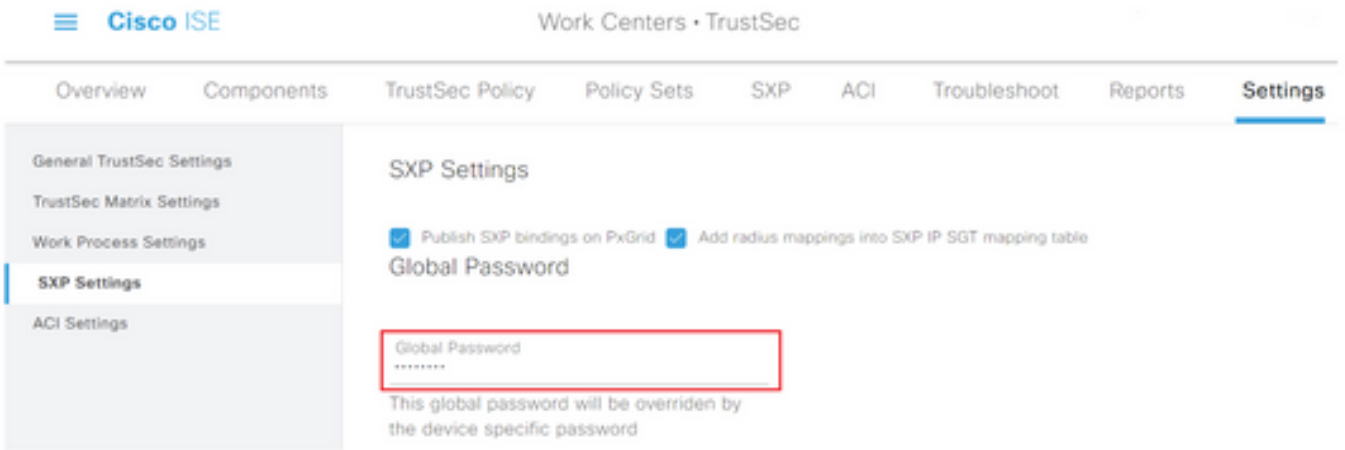
> لمعال زكرم في ددحو رسيال ىلعأل نكرلا في ةدوجوم رطسأ ةثالث ةنوقيأ ددح. 1 ةوطخال  
تادادع | TrustSec >

SXP تادادع | ءحفص رقنا. 2 ةوطخال

pxGrid ىلع SXP طباور رشن رايتخال ءناخ ددح، IP-SGT تانبيعت رشنل. 3 ةوطخال



ةمء رورم ةملك تحت SXP تاداءءل ةضارتفا رورم ةملك ففرءب مق .(ةرءاءءا) 4 ةوطءلا

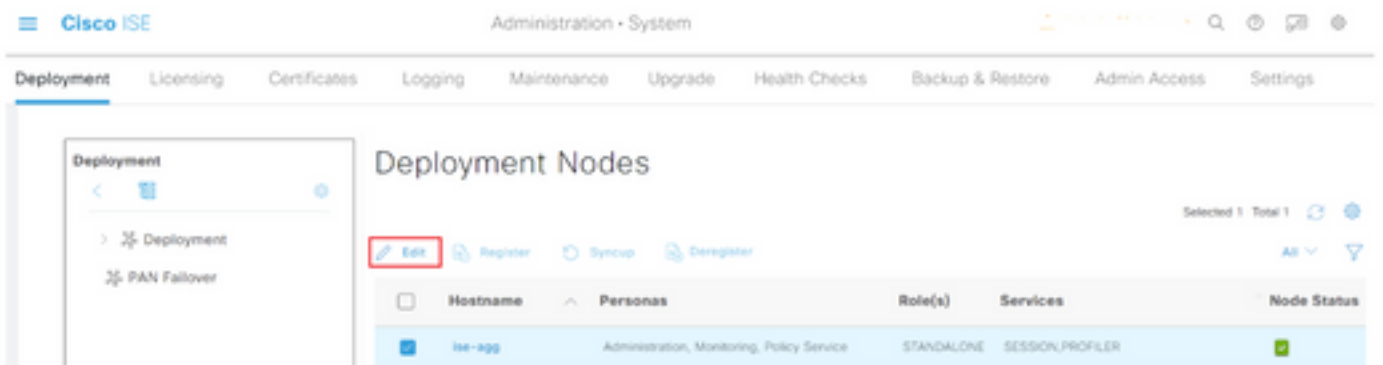


.ظفء قوف رقناو لفسأل ررمرءلاب مق .5 ةوطءلا

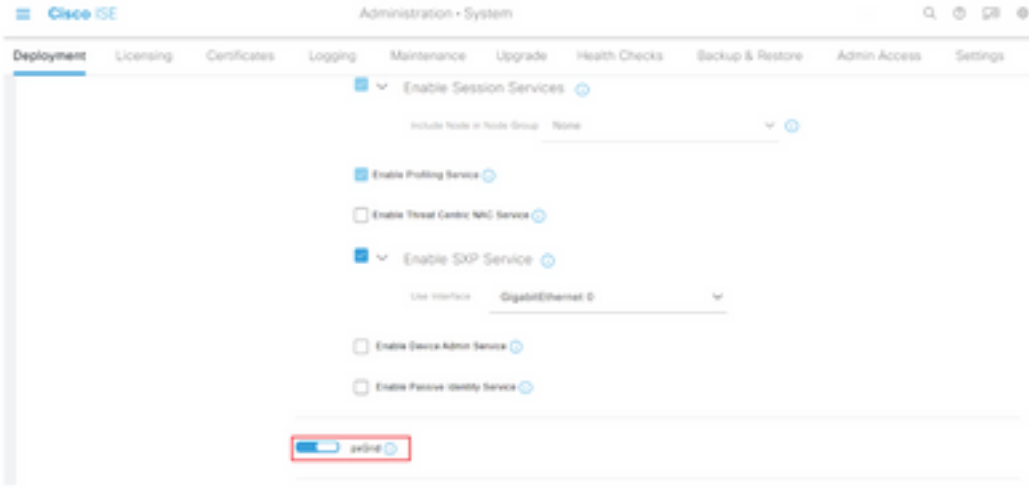
ءءءءلا ةءقء فف pxGrid نءكمء

ءراءءلا فف ءءو رسءلا ةءولءلا ةءوازلا فف ءءوءوملا ةءالءلا طوءءلا ءنوءفءء ءء .1 ةوطءلا  
> رءننلا > ماظننلا >

.ررءء قوف رقناو اءنءوءء ءرءء ءءلا ةءقءلا ءء .2 ةوطءلا



.pxGrid راءء ءوءوملا رءلا رقنا، pxGrid نءكمءءلا .3 ةوطءلا

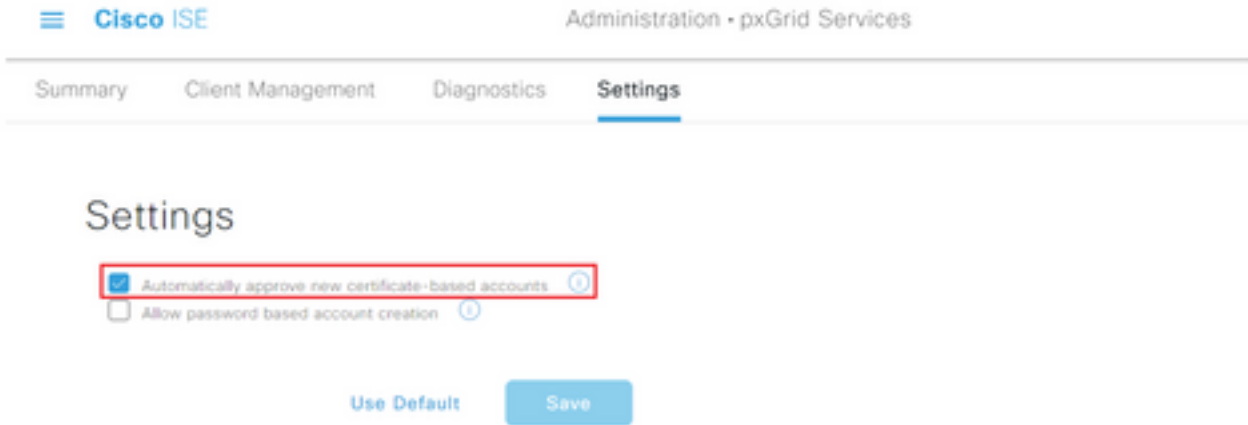


ظفح قوف رقن او لفسألأ ىلإ ريرم تلاب مق 4. ةوطخل

## pxGrid ل ىئاقلتلا دامتعالا

> ةرادإ ددحو ىرسىلا ةىولعل ةىوازلا ىف ةدوجوم رطسأ ةثالث ةنوقىأ ىلإ لقتنا 1. ةوطخل  
تاداعإ > pxGrid تامدخ

PXgrid ءالمع نم pxGrid لاصتاتابلط ىلع ىئاقلتلا ISE قفاوى ال، اىضارتفا 2. ةوطخل  
ىلع ةىئاقلتلا ةقفاوملا رايئتخالا ةناخ دىدحت قىرطنع دادعإلا اذه نىكمت بىجى كلذل، ددجل  
ةداهش ىلإ ةدنتسمل ةدىجل تابساحلا



ظفح ةقطق 3. ةوطخل

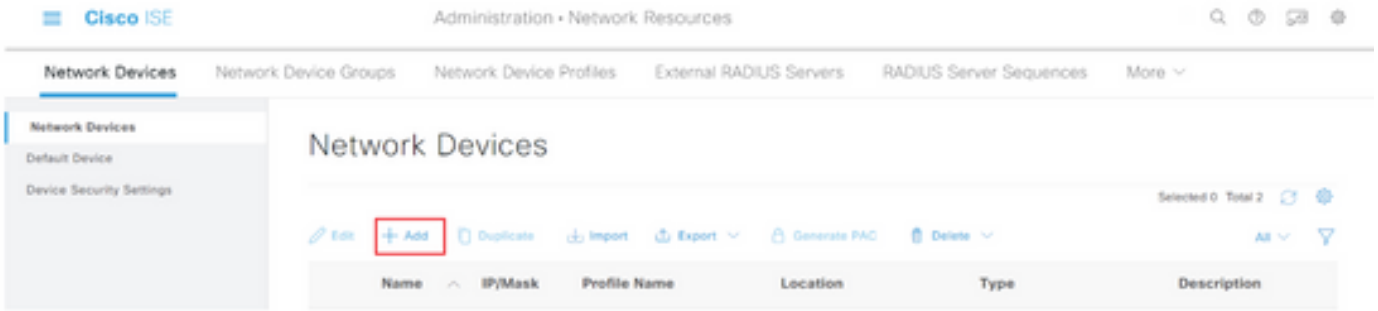
## ةكبشلا ةزهجال TrustSec تاداعإ

بىجى، اهىلع TrustSec نىكمت مت ىتلا ةزهجال نم تابلطلا ةجلالم نم Cisco ISE نىكمت ىكى  
Cisco ISE ىف اهىلع TrustSec نىكمت مت ىتلا ةزهجال دىدحت ىكىلع

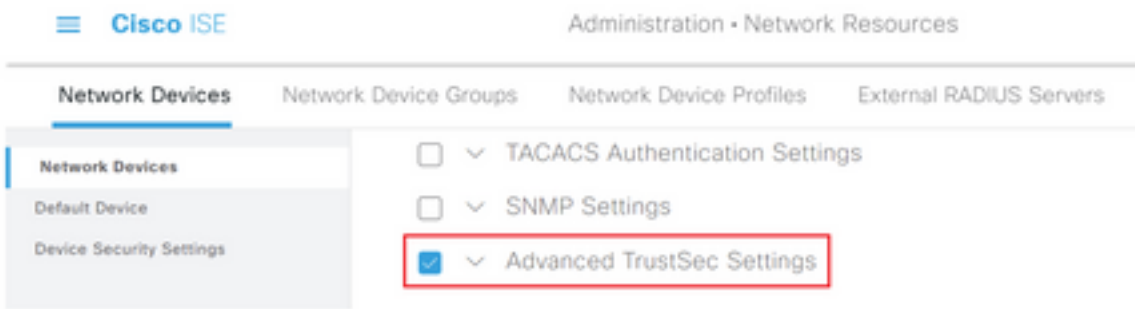
> ةرادإ ىلع ددحو رسىلا ةىولعل نكرلا ىف ةدوجوملا ةثالثلا طوطخل ىلإ لقتنا 1. ةوطخل  
ةكبشلا ةزهجال > ةكبشلا دراوم

ةفاضإ+ ةقطق 2. ةوطخل

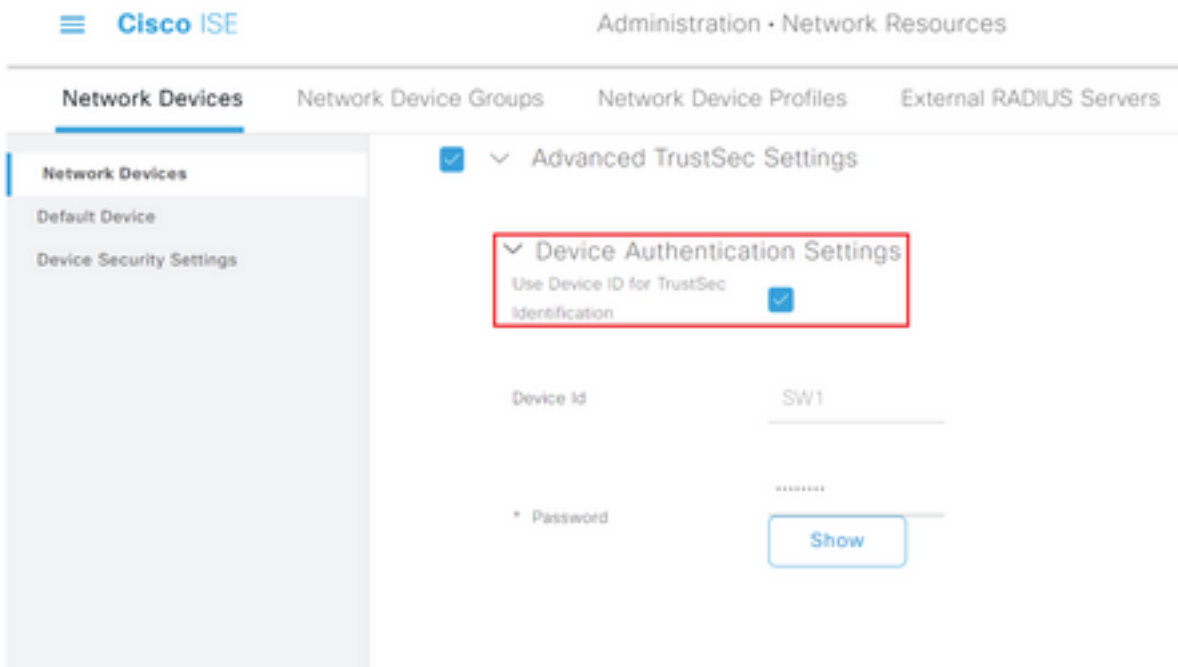




RADIUS. ةقداصم تادادع| يف و ةكبشلا ةزهجأ مسق يف ةبولطملا تامولعمل لخدأ. 3 ةوطخل  
TrustSec. ل نكمم زاهج نيوكتل ةمدقتملا TrustSec تادادع| رايتخاله ةناخ ددح. 4 ةوطخل

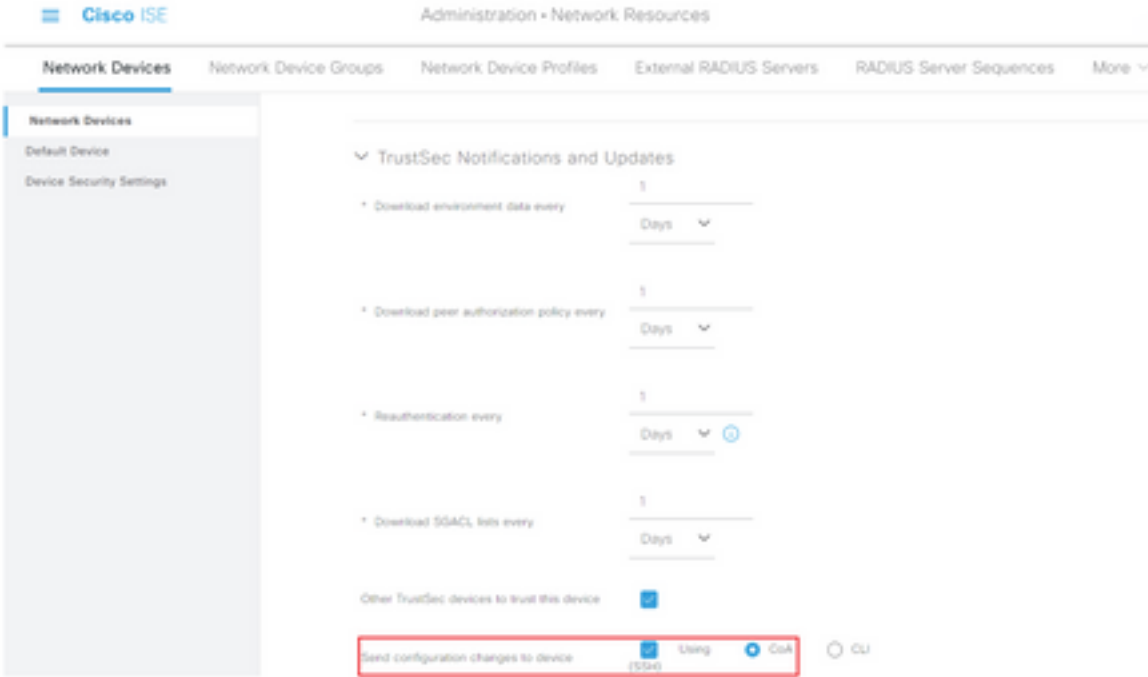


مسا ميمعتل TrustSec فيرعتل زاهجل فرعم مادختسا رايتخاله ةناخ لىل رقنا. 5 ةوطخل  
رورملا ةملك ل قح يف رورم ةملك لخدأ. ايايقلت ةكبشلا ةزهجأ مسق يف دورسلا زاهجل



مظالم "cts credentials id <id> password" رمأل عم رورملا ةملك و فرعمل قباطتي نأ بجي: ةظالم  
ل وحمل لىل اقحاله نيوكت مت يذال <pw>".

لاسرا نم ISE نكمتي شيحب زاهجل لىل نيوكتل تاريخيغت لاسرا رايتخاله ةناخ ددح. 6 ةوطخل  
زاهجل لىل TrustSec نم CoA تامالعه



نام ألة وعمجم عمال ع نبيعت تاتي دحت رشن دنع زاهجال اذه نيمضت راي تخالال ةناخ ددح . 7 ةوطخلال

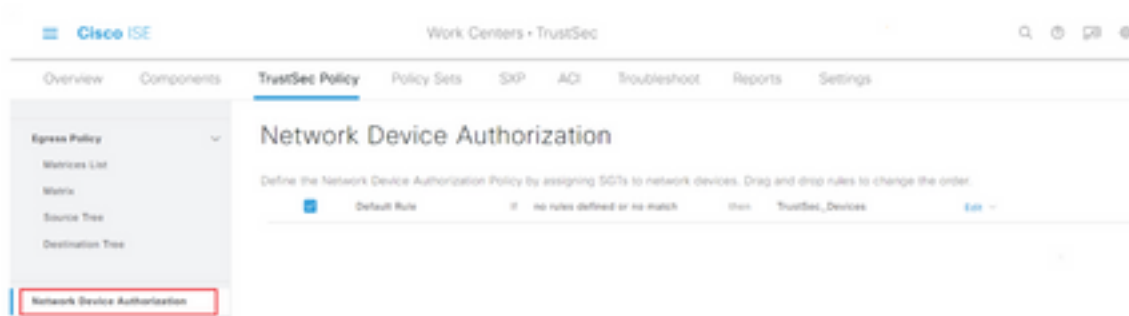
تاغوسم لمعمتسم لال ، ةأدا ةكبشلال نم لئكشلال ررحي ISE تكترت in order to تلخد . 8 ةوطخلال  
لال في ةم لك enable ، راي تخالال دوزي . لاجم ةم لك بولس EXEC و username بولس EXEC لال في  
لال . لاجم ةم لك بولس enable

TrustSec لاجم نم اعزج نوكت نأ دصقي يئلال يرخالال NADs عي مجل تاوطخلال ررك : ةظحالام

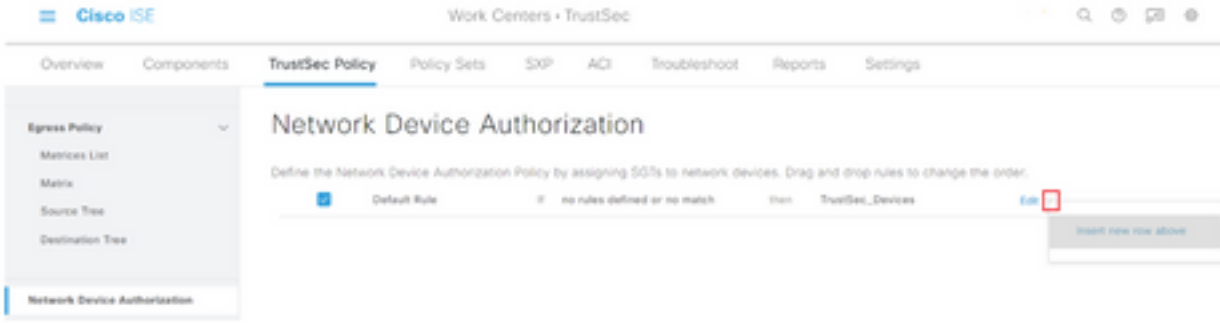
## ةكبشلال زاهج ضيوف

زكارم في ددحو رسي لال ةيولعلال ةيوازلال في ةدوجوملال ةثاللال طوطخلال ةنوقي أي ددح . 1 ةوطخلال  
TrustSec > TrustSec > لعملال

ةكبشلال زاهج ضيوفت لىل ع رقنا ، رسي ألال اعزجال في . 2 ةوطخلال

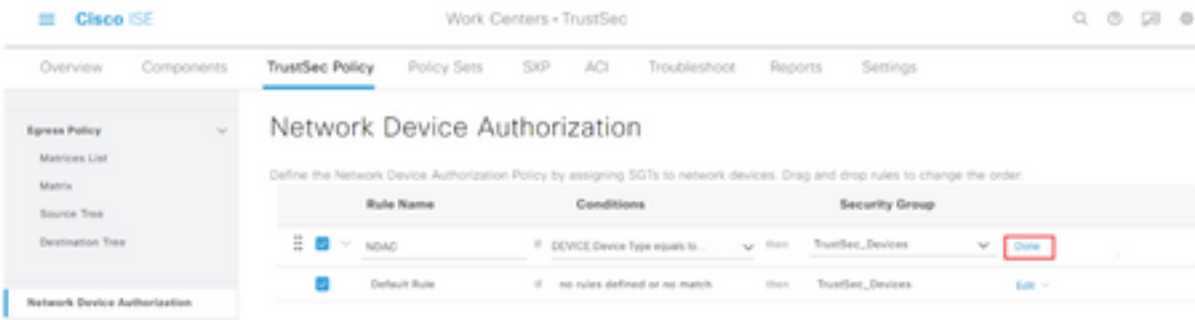


هالعا ديدج فص جارداو ريرحتلال ةرواجملا ةلدسنملا ةمئاقلال مدختسأ ، نيمي لال لىل . 3 ةوطخلال  
ةديدج NDA ةدعاق عاشنال



ةلدسنملا ةمئاقلا نم بسانملا بيقرلا دحو اهطورشو ةدعاقلا مسا ديحتب مق 4. ةوطخلا نامالا تاعومجم تحت

نيميللا يصقأ لىا مت ةقطق 5. ةوطخلا



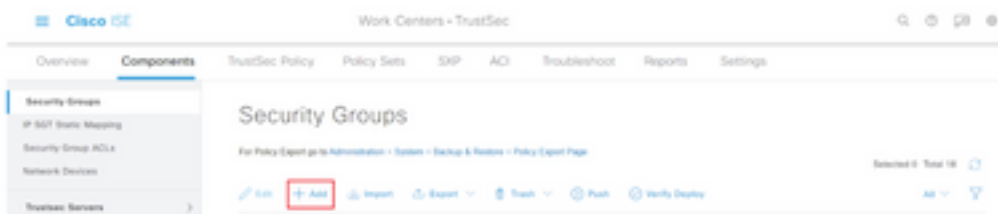
ظفح قوف رقناو لفسال ريرمتلاب مق 6. ةوطخلا

بيقر

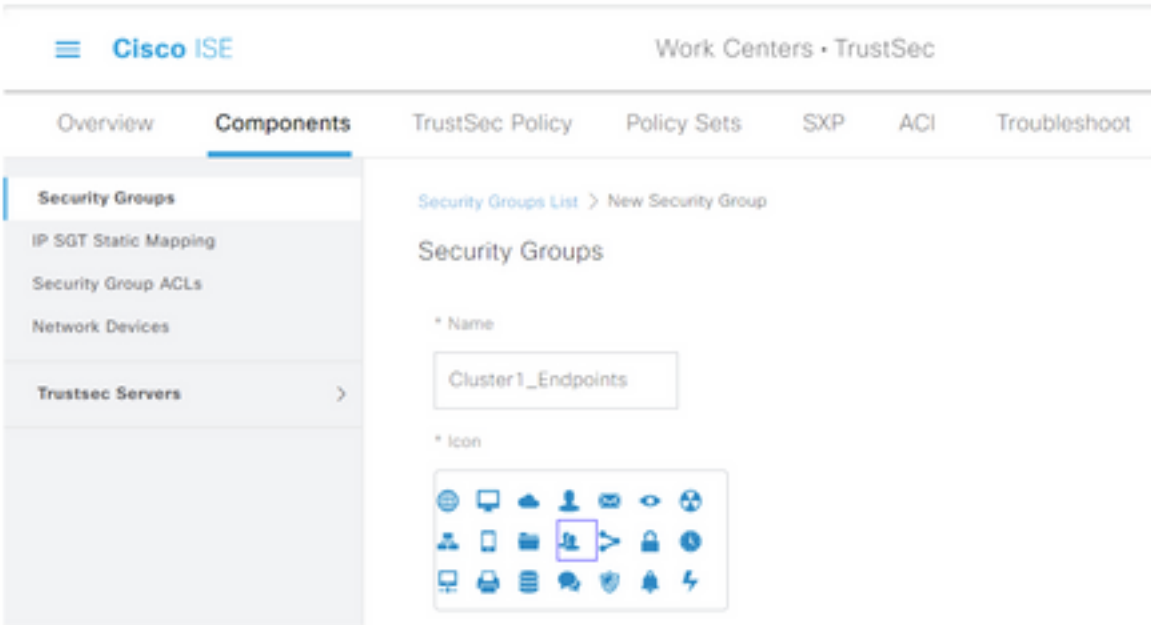
زكارم يف دحورسيالا لىعالا نكرلا يف ةدوجوملا ةثالثلا طوطخلا ةنوقيأ دح 1. ةوطخلا تانوكملا > TrustSec > لمعلا

نامالا تاعومجم عيسوتب مق ،رسيالا عزجال يف 2. ةوطخلا

ديج بيقر عاشنال ةفاضلا+ رقنا 3. ةوطخلا



ةبسانملا لوقحلا يف ةنوقيأ رتخاو مسالا لخدأ 4. ةوطخلا



زېږېمت ؤمالع ؤمېق لخدأو افسو هطعأ ،ايرايختخ | 5 ؤوطخلا

> لمعال زكارم لىل لوقتنا ،ايوډي زېږېمت ؤمالع ؤمېق لخدإ نم نكمتلا لجأ نم : ؤطخال  
مقرر لخدإ مدختسم لىل عېجې رايخل ددحو General TrustSec ناداع | > ناداع | TrustSec >  
ناملال ؤومجم ؤمالع مېقرت تحت ايوډي بېقرل

لاسرا قوف رقناو لفسأل ريرمتلاب مق . 6 ؤوطخلا

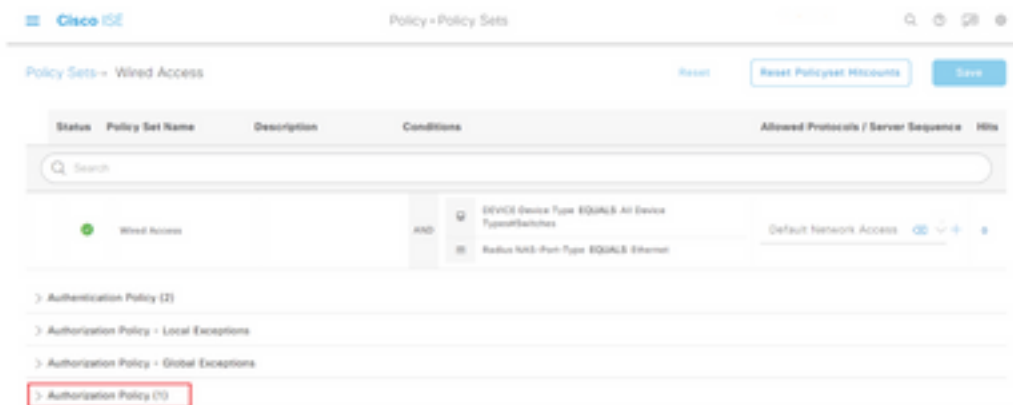
نېبولطم لىل عابقرل اعمجل تاوطلخال هذو ررك : ؤطخال

## لېوختلا ؤسايس

ي ف ددحو ىرسېلا ؤيولعل ؤيوازلا ي ف ؤدوجومال ؤثالثلا طوطخلال ؤنوق ي ددح . 1 ؤوطخلال  
تاسايسلال تاومجم > ؤسايسلال

ةبسانملا جهنلا ؤومجم ددح . 2 ؤوطخلال

لېوختلا جهن عيسوتب مق ،جهنلا ؤومجم نمض . 3 ؤوطخلال



ل.ي.وخت جهن عاشن رز قوف رقنا 4. ةوطخلا



Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Actions

ب.ي.ق.ر.ل.ا ددحو ةبولطم ال فيرعتل ا فامل و s/طرشل او ةءاقل ا مسا دي دحت ب مق 5. ةوطخلا  
ن.ا.م.ا.ل.ا تاعومجم تحت ةلدسننم ال ةمئاق ال نم بس انم ال

Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
On	Default Policy	www_802.1x	PermitAccess	Cluster1_Endpoints		

ظ.ف.ح. ةق.ط.ق.ط. 6. ةوطخلا

(ي.راي.خ) ISE ع.ي.م.ج.ت.ل.ا ةدق.ع. ي.ل.ع. ERS ن.ي.ك.م.ت

اهن ع مالع تسال انكمي (API) تاق.ي.ب.ط.ت. ةجمرب ةهجاو يه (ERS) ةي.ج.را.خ. ال RESTfull API ةمدخ  
ي.ض.ارت.فا.ل.ك.ش.ب. ERS ةمدخ لي.ط.ع.ت. م.ت.ي. ة.ع.وم.ج.م.ل.ا تاملوم ع ي.ل.ع. ل.وص.ح.ل.ل. WSA ةطساوب  
اذا (API) تاق.ي.ب.ط.ت.ل.ا ةجمرب ةهجاو نع مالع تسال اءالمعلل نكمي ،اهن.ي.ك.م.ت. درجم بو. ISE ي.ل.ع.  
ةفاضاو ISE ي.ل.ع. ةمدخلل نكمم تل. ISE ةدق.ع. ي.ل.ع. ERS لوؤسم ةعومجم ءاضع ا ةقداصمب اوماق  
ةي.ل.ل.ل.ا تاولط.خ.ل.ا ع.ب.ت.ا ،ة.ح.ي.ح.ص.ل.ا ةعومجم ال ي.ل.ع. باسح

> ةرادا ي.ل.ع. ددحو ىرس ي.ل.ع. ةي.وازل ي.ف. ةدوجوم ال ةثال.ل.ا طوط.خ.ل.ا ةنوقي ا ددح 1. ةوطخلا  
ت.ا.د.ا.ء.ال.ا > ماظن ال

ERS. ت.ا.د.ا.ء.ال.ا ي.ل.ع. رقنا ،ىرس ي.ل.ع. ةحول ال ي.ف. 2. ةوطخلا

The screenshot shows the Cisco ISE Administration - System Settings page. The left sidebar contains various settings categories like Client Provisioning, Security Settings, Posture, etc. The main content area is titled 'ERS Settings' and includes a 'General' section with a description of ERS and a 'ERS Setting for Administration Node' section where the 'Enable ERS' radio button is selected.

ة.ب.ا.ك.ل.ا/ةءارق.ل.ل. ERS ن.ي.ك.م.ت. راي.خ.ل.ا ددح 3. ةوطخلا

OK. م ادختساب ديكأتو ظفح قوف رقنا 4. ةوطخلا

## (يراي تخ) ESR ةرادا ةومجم لىل مدختسم ةفاضل

> ةرادا ددحو ىرسىلا ةيولعل ةيوازلا يف ةدوجوملا ةثالثلا رطسألا ةنوقىأ ددح 1. ةوطخلا  
لوؤسملا لوصو > ماظن

Admin Users قوف رقناو Administrators عيسوتب مق ،رسىألا عزجلا يف 2. ةوطخلا

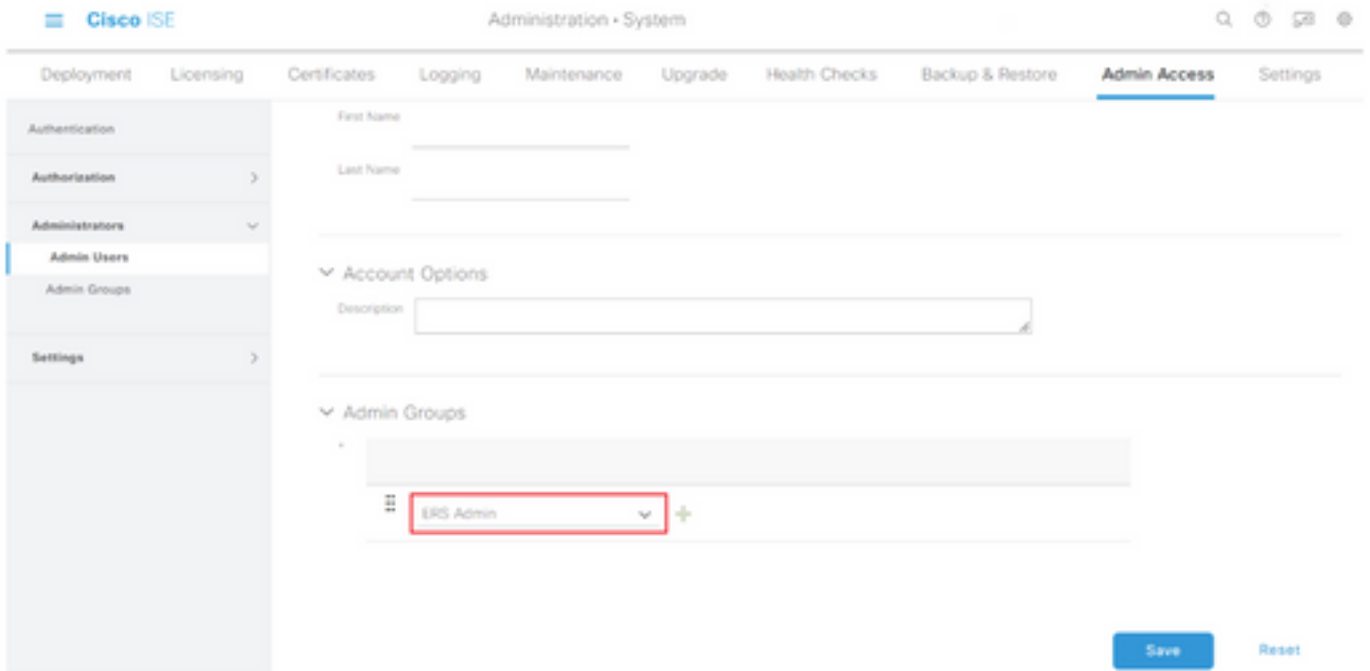
ةلدسنملا ةمئاقلا نم لوؤسملا مدختسم ددحو ةفاضل+ قوف رقنا 3. ةوطخلا

The screenshot shows the Cisco ISE Administration - System interface. The top navigation bar includes 'Deployment', 'Licensing', 'Certificates', 'Logging', 'Maintenance', 'Upgrade', 'Health Checks', 'Backup & Restore', 'Admin Access', and 'Settings'. The 'Admin Access' tab is active. The left sidebar has 'Authentication', 'Authorization', 'Administrators', 'Admin Users', 'Admin Groups', and 'Settings'. The 'Administrators' section is expanded, and 'Admin Users' is selected. The main content area displays the 'Administrators' page with a table containing one entry: 'Default Admin User' with 'Super Admin' as the group. A dropdown menu is open over the table, showing options: 'Create an Admin User' and 'Select from Network Access Users'.

ةبسانملا لوقحلا يف رورم ةملكو مدختسم مسا لخدأ 4. ةوطخلا

The screenshot shows the Cisco ISE Administration - System interface. The top navigation bar includes 'Deployment', 'Licensing', 'Certificates', 'Logging', 'Maintenance', 'Upgrade', 'Health Checks', 'Backup & Restore', 'Admin Access', and 'Settings'. The 'Admin Access' tab is active. The left sidebar has 'Authentication', 'Authorization', 'Administrators', 'Admin Users', 'Admin Groups', and 'Settings'. The 'Admin Users' section is expanded, and 'Admin Users' is selected. The main content area displays the 'Admin User' configuration page. The configuration fields include: Name (WSA), Status (Enabled), Email, External (unchecked), Read Only (unchecked), Inactive account never disabled (unchecked), Password, and Re-Enter Password.

ERS لوؤسم ديدحتل ةلدسنملا ةمئاقلا مدختسأ ،ةرادال تاومجم لقح يف 5. ةوطخلا



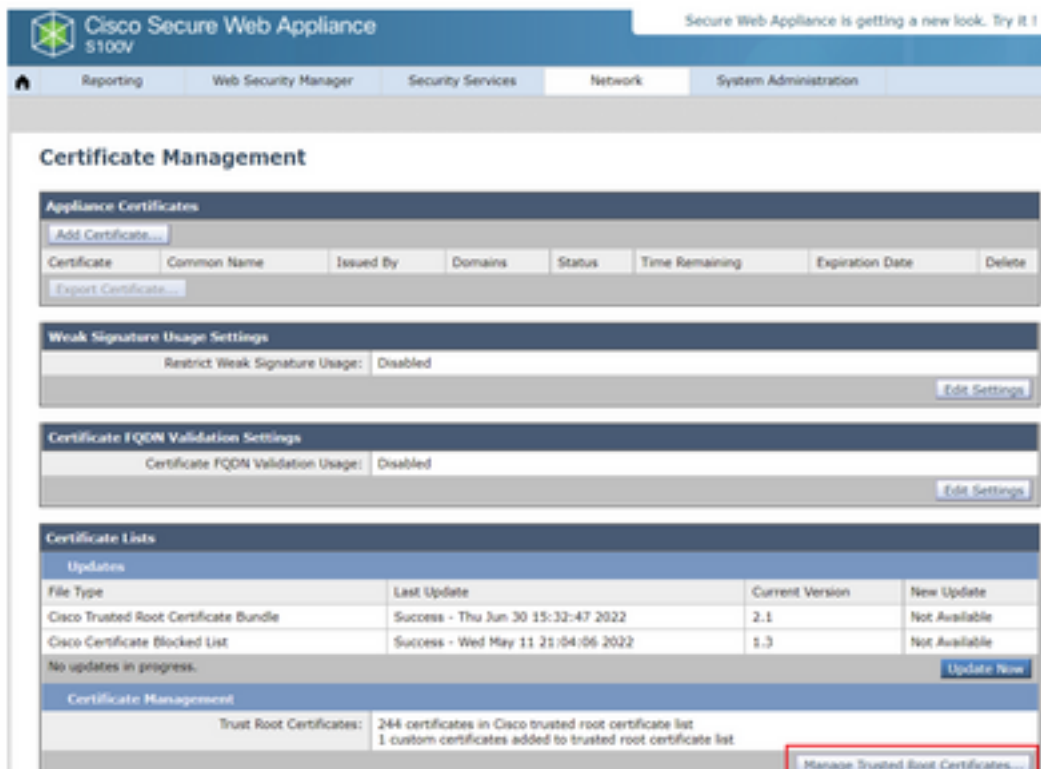
طفح ةق قوط 6. ةوطخل

## نمآلا ببول زاغ نيوكت

رذجل ةداهشلا

ISE و WSA نيپ لاصتاللة قثلل رذكل يلخاد ةداهش عجرم مدختسي لماكلتلا ميمصت ناك اذا ني زاهجال الك ىلع هذه رذجل ةداهش تيبتت بجيف

اهب قوثلما رذجل ةداهش ةرادىل عرقناو ةداهشلا ةرادىل > ةكپشلا ىللقنا 1. ةوطخل ةق قوصم عجرم ةداهش ةفاضل



## داري تس | قوف رونا 2. ةوطخل



رقناو هؤاشن | مت يذلا رذجل ا قوصم ا عجرم ا ع قوم ديحت ل فلم رايخ | قوف رونا 3. ةوطخل  
لاسرا قوف

ىرخ أرم لاسرا قوف رونا 4. ةوطخل

تاريغت ل ديكت أ رونا، ىنم يلا ةيولعل ا ةيوازلا ي 5. ةوطخل



ىرخ أرم تاريغت ل ذيفنت قوف رونا 6. ةوطخل

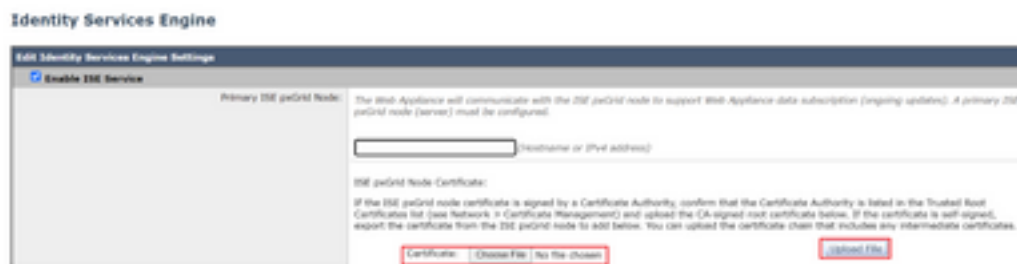
## pxGrid ةداهش

نيوكت نم عزجك PXgrid ةطساوب مادختس ل ا ةداهش ل اوح ي تافم ل ا جوز ءاشن | مت ي WSA، ي ISE. تامدخ

ةيولعل ا ةمدخ كرحم > ةكبش ل ا ل لقتنا 1. ةوطخل

تادادع ل ا ريرحت و نيكت ىل ع رونا 2. ةوطخل

رقناو هؤاشن | مت يذلا رذجل ا قوصم ا عجرم ا ع قوم ديحت ل فلم رايخ | قوف رونا 3. ةوطخل  
فلم ل ا ليحت قوف



بج ي. مسق ل ا اذه ي pxGrid ISE ةداهش ل ليحت و هو ءاشن نيوكت ا طخ كانه : ةطخال  
pxGrid ISE ةداهش ل ل قح ىل رذجل ا قوصم ا عجرم ل ا ةداهش ل ليحت

مت نيذلل ا حتافم ل ا ةداهش ل ا مادختس | دح، بيولا زاخ ل ليحت ةداهش مسق ي 4. ةوطخل  
امهؤاشن |



**Web Appliance Client Certificate:** For secure communication between the Web Appliance and the ISE pxGrid servers, provide a client certificate. This may need to be uploaded to the ISE pxGrid node(s) configured above.

Use Uploaded Certificate and Key

Certificate:  No file chosen

Key:  No file chosen

Key is Encrypted

No certificate has been uploaded.

Use Generated Certificate and Key

ةبولطملا ةداهشلا لوقح لمكأو ديدج حاتفمو ةداهش عاشنإ رز رقنا 5 ةوطخلا

**Generate Certificate and Key** [X]

Common Name:

Organization:

Organizational Unit:

Country:

Duration before expiration:  months

Basic Constraints:  Set X509v3 Basic Constraints Extension to Critical

ةداهشلا عيقوت ليزنت بلط يلع رقنا 6 ةوطخلا

مت اذا ISE نيوكت يف تاريخي غتلا ذيفنتل لاسرل رزلا ديدجت نسحتسملا م :ةظحالم يتلا ةداهشلا وحياتافملا دوقف نكمي ،تاريخي غتلا لاسرل لبق ةلهملل لمعلا ةسلج كرت CSR ليزنت مت اذا يتح ،اهؤاشنإ مت

ةداهشلا عقوم ديدحتل فلم راي تخا قوف رقنا ،كب صاخلا CA عم CSR عيقوت دعب 7 ةوطخلا

**Web Appliance Client Certificate:** For secure communication between the Web Appliance and the ISE pxGrid servers, provide a client certificate. This may need to be uploaded to the ISE pxGrid node(s) configured above.

Use Uploaded Certificate and Key

Certificate:

Key:

Key is Encrypted

No certificate has been uploaded.

---

Use Generated Certificate and Key

Common name: wsa.securitylab.net  
 Organization: Cisco  
 Organizational Unit: Security  
 Country: SE  
 Expiration Date: May 10 19:19:26 2024 GMT  
 Basic Constraints: Not Critical

[Download Certificate...](#) | [Download Certificate Signing Request...](#)

Signed Certificate:

To use a signed certificate, first download a certificate signing request using the link above. Submit the request to a certificate authority, and when you receive the signed certificate, upload it using the field below.

Certificate:

فلم ل لېمحت قوف رقنا 8 ةوطخ ل

مازتلاو لاسرا 9 ةوطخ ل

نم آل بېولا زاغ ىل ع ERS و SXP نې كم ت

ERS و SXP نم لك ل نې كم ت ل رارزا رقنا 1 ةوطخ ل

ISE SOAP Exchange Protocol (SXP) Service: Enabling the service, Web Appliance will retrieve SXP Binding Topic from ISE Services.

Enable ISE External Restful Service (ERS)

The Web Appliance retrieves Active Directory groups, and local ISE groups from ISE using the ERS. If you are configuring the Web Appliance's policies using Active Directory groups, or in combination with Secure Group Type (SGT), you should enable ERS.

ىل ع اهنې وكت مت ىت ل م دخت س م ل تام ول عم ل خ دأ، ERS لوؤسم تاغ وسم ل قح ىف 2 ةوطخ ل ISE.

م ىت ل تام ول عم ل ثرت ل ISE pxGrid ةدق ع ل هس فن م داخ ل م س ال ع ب ر م ل ددح 3 ةوطخ ل . كانه ةبول ط م ل تام ول عم ل ل خ داف ، ال او . اق ب س م اهنې وكت

Enable ISE External Restful Service (ERS)

ERS Administrator Credentials

Username:

Password:

ERS Servers

Server name same as ISE pxGrid Nodes

Primary:  (Hostname or IPv4 address)

Secondary (Optional):  (Hostname or IPv4 address)

Port:  (Enter the port number specified for ERS in ISE)

مازتلاو لاسرا 4 ةوطخ ل

فېرعت ل فېرعت فلم

فلم عاشن بجي WSA، تاسايس في ISE ةومجم تامولعم وأ نامأل ةومجم تامالع مادختس ال ةيفافش ب نيمدختس مل فيرعتل ةلبيسوك ISE مدختسي فيرعت

فيرعتل تافيصوت > ةقداصملا > بيولا نامأ ريدم يل لقتنا 1. ةوطخل

فيرعت فيصوت ةفاضل عل رقتنا 2. ةوطخل

ايرايخا فصوو امسا لخدأ 3. ةوطخل

فيرعت رايخال ةلدسنملا ةمئاقلا مدختسأ، ةقداصملاو فيرعتل امسق في 4. ةوطخل ISE. مادختساب ةيفافش ب نيمدختس مل

#### Identification Profiles: Add Profile

Client / User Identification Profile Settings	
<input checked="" type="checkbox"/> Enable Identification Profile	
Name:	<input type="text" value="ISE Profile"/> <small>(e.g. my IT Profile)</small>
Description:	<input type="text" value="Identification profile for ISE integration."/> <small>(Maximum allowed characters 256)</small>
Insert Above:	<input type="text" value="2 (Global Profile)"/>

User Identification Method	
Identification and Authentication:	<input type="text" value="Transparently identify users with ISE"/>
Fallback to Authentication Realm or Guest Privileges:	<input type="text" value="Support Guest Privileges"/> <small>Authorization of specific users and groups is defined in subsequent policy layers (see Web Security Manager &gt; Decryption Policies, Routing Policies and Access Policies).</small>

Membership Definition	
<small>Membership is defined by any combination of the following options. All criteria must be met for the policy to take effect.</small>	
Define Members by Subnet:	<input type="text"/> <small>(examples: 20.1.1.0, 20.1.1.0/24, 20.1.1.1-50, 2001:420:80:2::5, 2000:db8::1-2000:db8::60)</small>
Define Members by Protocol:	<input checked="" type="checkbox"/> HTTP/HTTPS
<a href="#">Advanced</a> Define additional group membership criteria.	

مازلالو لاسرا 5. ةوطخل

بيقرلا لعل ةمئاقلا زيمرتلا كفايس

ريفتل كفايس > بيولا تاسايس > بيولا نامأ ةرادا يل لقتنا 1. ةوطخل

جهن ةفاضل قوف رقتنا 2. ةوطخل

ايرايخا فصوو امسا لخدأ 3. ةوطخل

ةلدسنملا ةمئاقلا مدختسأ، نيمدختس مل او فيرعتل تافيصوت امسق في 4. ةوطخل رثكأ وأ دحاو فيرعت فيصوت ديدحت رايخال

فلم مسارا رايخال ةلدسنملا ةمئاقلا مدختسأ، فيرعتل تافيصوت امسق في 5. ةوطخل ISE. فيرعت

ةددحملا تاعومجملا ددح، ةدمتعمل تاعومجملاو نومدختس مل امسق في 6. ةوطخل نيمدختس مل او

**Policy Member Definition**

Membership is defined by the combination of the following options. All criteria must be met for the policy to take effect.

Identification Profiles and Users:

Identification Profile	Authorized Users and Groups	Add Identification Profile
ISE Profile	<input type="radio"/> All Authenticated Users <input checked="" type="radio"/> Selected Groups and Users (2) ISE Secure Group Tags: No tags entered ISE Groups: No groups entered Users: No users entered <input type="radio"/> Guests (users failing authentication)	<input type="button" value="Add Identification Profile"/>

Authentication information may not be available at HTTPS connection time. For transparent proxy traffic, user agent information is unavailable for decryption policies.

[Advanced](#) Define additional group membership criteria.

ة.نمآل ISE ةومجم تامالع راجب دوجومل ايبعش التا طابترالال قوف رقنا 7. ةوطخلال

نمي ىل دوجومل عبرملا دح ،ةنمآل ةومجمل زييمت ةمالع نع ثحبلال مسق يف 8. ةوطخلال ةفاضل قوف رقناو بولطملال بيقرلال

**Authorized Secure Group Tags**

Use the search function below to add Secure Group Tags. To remove Secure Group Tags from this policy, use the Delete option.

1 Secure Group Tag(s) currently included in this policy.

Secure Group Tag Name	SGT Number	SGT Description	Delete
Cluster1_Endpoints	111	Endpoints residing in ISE Cluster-1	<input type="checkbox"/>

**Secure Group Tag Search**

Enter any text to search for a Secure Group Tag name, number, or description. Select one or more Secure Group Tags from the list and use the Add button to add to this policy.

0 Secure Group Tag(s) selected for Add

Secure Group Tag Name	SGT Number	SGT Description	Select
Production_Servers	11	Production Servers Security Group	<input type="checkbox"/>
Point_of_Sale_Systems	10	Point of Sale Security Group	<input type="checkbox"/>
Test_Servers	13	Test Servers Security Group	<input type="checkbox"/>
Development_Servers	12	Development Servers Security Group	<input type="checkbox"/>
BYOD	15	BYOD Security Group	<input type="checkbox"/>
PCI_Servers	14	PCI Servers Security Group	<input type="checkbox"/>
Guests	6	Guest Security Group	<input type="checkbox"/>
ANY	65535	Any Security Group	<input type="checkbox"/>
Unknown	0	Unknown Security Group	<input type="checkbox"/>
Network_Services	3	Network Services Security Group	<input type="checkbox"/>
TrustSec_Devices	2	TrustSec Devices Security Group	<input type="checkbox"/>
Cluster1_Endpoints	111	Endpoints residing in ISE Cluster-1	<input checked="" type="checkbox"/>
Employees	4	Employee Security Group	<input type="checkbox"/>

عجري نأ م ةققط 9. ةوطخلال

مزلتلال لاسرا 10. ةوطخلال

لّ دبلال نيوكت

AAA

```

aaa new-model

aaa group server radius ISE
  server name ise01-cl1
  server name ise02-cl1
  ip radius source-interface Vlan50

aaa authentication dot1x default group ISE
aaa authorization network ISE group ISE
aaa accounting update newinfo periodic 2440
aaa accounting dot1x default start-stop group ISE

aaa server radius dynamic-author
  client 10.50.50.120 server-key Cisco123
  client 10.50.50.121 server-key Cisco123
  auth-type any

radius server ise01-cl1
  address ipv4 10.50.50.121 auth-port 1812 acct-port 1813
  pac key Cisco123
radius server ise02-cl1
  address ipv4 10.50.50.120 auth-port 1812 acct-port 1813
  pac key Cisco123

```

## كيسورت

```

cts credentials id SW1 password Cisco123 (This is configured in Privileged EXEC Mode)
cts role-based enforcement

```

```

aaa authorization network cts-list group ISE
cts authorization list cts-list

```

## ةحصلال نم ققحتلال

ةياهنلال ةطقن لىل ISE نم بيقرلال ةمهم

ةقداصملا حاجن دعب اهل بيقرن نيي عت مت 1 ISE ةومجم نم ةياهن ةطقن ةيؤر انه كنكمي  
ضيفوتلالو:

Identity	Endpoint ID	Endpoint Profile	Authentication Policy	Authorization Policy	Authorization Profile	IP Address	Security Group	Server
10.50.50.120	14.02.001	IP Device	Wind Access -->	Wind Access -->	Permissive	10.50.50.12	Client_Endpoint	ise01-cl1

ةقداصملا حاجن دعب اهل بيقرن نيي عت مت 2 ISE ةومجم نم ةياهن ةطقن ةيؤر انه كنكمي  
ضيفوتلالو:

Identity	Endpoint ID	Endpoint Profile	Authentication Policy	Authorization Policy	Authorization Profile	IP Address	Security Group	Server
10.50.50.121	14.02.001	Microsoft Work	Wind Access -->	Wind Access -->	Permissive	10.50.50.12	Client_Endpoint	ise02-cl1

## SXP تانبيعت

فرعتلال متي ISE، عيمجت ةدقو ةومجملا ماظنل ISE دقع نبي SXP لاصتلا نيكم تل ارظنو  
SXP لالخن نم ISE عيمجت ةطساوب هذه SGT-IP تانبيعت لىل

Work Centers - TrustSec

Overview Components TrustSec Policy Policy Sets SXP AD Troubleshoot Reports Settings

All SXP Mappings

IP Address	SGT	VN	Learned From	Learned By	SXP Domain	PDNs Involved
10.50.50.112	TrustSec_Device (20000)		10.50.50.121_10.50.50.0	SXP	default	10.50.50.0
10.50.50.112	TrustSec_Device (20000)		10.50.50.122_10.50.50.7	SXP	default	10.50.50.0
10.50.50.121	Cluster_Endpoints (1110000)		10.50.50.121_10.50.50.0	SXP	default	10.50.50.0
10.50.50.122	Cluster_Endpoints (2220000)		10.50.50.122_10.50.50.7	SXP	default	10.50.50.0

نم PxGrid ربع WSA ىلإ ،ةفلتخلم ال ISE اتاعومجم نم ،هذه SXP تانييعة لاسرا لك لذ دع ب متي ISE عيجمت ةدقع لال خ

```
wsa2.securitylab.net> isedata
Choose the operation you want to perform:
- STATISTICS - Show the ISE server status and ISE statistics.
- CACHE - Show the ISE cache or check an IP address.
- SGTs - Show the ISE Secure Group Tag (SGT) table.
- GROUPS - Show the ISE Groups table.
[>] cache

Choose the operation you want to perform:
- SHOW - Show the ISE IP cache.
- CHECKIP - Query the local ISE cache for an IP address
[>] show
IP                username                               SGT#  Port Range
10.50.50.11      isesxp_10.50.50.122_sgt222_10.50.50.13 222   -
10.50.50.12      isesxp_10.50.50.121_sgt111_10.50.50.12 111   -
```

بيقرلا ىل ع مئاقلا تاسايسلا قيبتت

اهب ةصاخلا تاسايسلا عم قباطت يتلا ةفلتخلم ةياهنلا طاقن ىرت نأ انه كنكمي اهلجريس ىلإ ادانتسا رورملا ةكرح عنم متي

ISE 1 ةعومجم ىلإ يمتنت يتلا ةياهنلا ةطقن

Notification: Policy: Destination x +

← → ↻ [bbc.com](https://bbc.com)

**This Page Cannot Be Displayed**

Based on your organization's access policies, access to this web site ( <https://bbc.com/> ) has been blocked.

If you have questions, please contact your organization's network administrator and provide the codes shown below.

Date: Thu, 14 Jul 2022 14:28:16 CEST  
 Username: isesxp\_10.50.50.121\_sgt111\_10.50.50.12  
 Source IP: 10.50.50.12  
 URL: GET https://bbc.com/  
 Category: Block URLs CL1  
 Reason: UNKNOWN  
 Notification: BLOCK\_DEST

Results

Displaying 1 - 50 of 137 items. Items Displayed: 50

Time (GMT +02:00) Website (source) Display All Details... Disposition Bandwidth User / Client IP

14 Jul 2022 14:28:17	<a href="https://bbc.com/443/television">https://bbc.com/443/television</a> CONTENT TYPE: - URL CATEGORY: Block URLs CL1 DESTINATION IP: DETAILS: Decryption Policy: 'ISE_Cluster1', WBSA: No Score, Malware Analytics File Verdict: -	Block - URL Cat	0B	isesxp_10.50.50.121_sgt111_10.50.50.12 (Identified by ISE) 10.50.50.12
----------------------	--	-----------------	----	--

## ISE 2 ةوعومجم لىل يمتنت يتل اةهانل اةقون



### This Page Cannot Be Displayed

Based on your organization's access policies, access to this web site ( https://www.facebook.com/ ) has been blocked.

If you have questions, please contact your organization's network administrator and provide the codes shown below.

Date: Thu, 14 Jul 2022 14:23:58 CEST  
Username: isesxp\_10.50.50.122\_sgt222\_10.50.50.13  
Source IP: 10.50.50.13  
URL: GET https://www.facebook.com/  
Category: Block URLs CL2  
Reason: UNKNOWN  
Notification: BLOCK\_DEST

Time (GMT +02:00)	Website (count)	Disposition	Bandwidth	User / Client IP
14 Jul 2022 14:23:58	https://www.facebook.com/43/revision.js CONTENT TYPE: ... URL CATEGORY: Block URLs CL2 DESTINATION IP: ... DETAILS: Decryption Policy: 'ISE_Cluster2', WBS: No Score, Malware Analysis File Verdict: ...	Block - URL Cat	0B	isesxp_10.50.50.122_sgt222_10.50.50.13 (Identified by ISE) 10.50.50.13

## ةلص تاذا تامولعم

- [Identity Service Engine ةيوهلا ةمدخو بيولوا نامأ زاها لمكات لىلد](#)
- [TrustSec تامدخل ISE عم WSA لمكات نيوكت](#)
- [Cisco، نم ةيوهلا تامدخ كرحم لوؤسم لىلد](#)
- [Cisco Secure Web Appliance ل Cisco AsyncOS 14.5 ل مدختس مل ا لىلد](#)

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 ةلخت. فرتمة مچرت مء دقء ةل ةل ةفارتحال ةمچرتل عم لالحل وه  
ىل إأمءءاد ءوچرلاب ةصوء و تامةرتل هذه ةقء نء اهءل وئس م Cisco  
Systems (رفوتم طبارل) ةلصلأل ةزءل ءنل دن تسمل