

نمآ بيو زاهج عم ةددعتم لال ISE تاعومجم جمم TrustSec لال ةدنتسم لال جهنلل

تايوت حملال

[عمدقم لال](#)

[ةيساس الال تابلطت لال](#)

[تابلطت لال](#)

[عمدختسم لال تانوك لال](#)

[دويقل لال](#)

[ةكبش لال يطيطخت لال مسر لال](#)

[نويوكت لال](#)

[ISE نويوكت](#)

[SXP نويوكت](#)

[عمومجم لال ماظن دقع لال ع SXP نويوكت](#)

[عمجم لال دقع لال ع SXP نويوكت](#)

[عمجم لال دقع لال ع pxGrid نويوكت](#)

[pxGrid لال يئاقولت لال دامت لال](#)

[ةكبش لال ةزهجال TrustSec تاداع لال](#)

[ةكبش لال زاهج ضيوفت](#)

[بيقر](#)

[لليوخت لال ةسايس](#)

[\(يراي تخا\) ISE عمجم لال دقع لال ع ERS نويوكت](#)

[\(يراي تخا\) ESR ةرادا عمومجم لال مدختسم ةفاضا](#)

[نمآ لال بيولا زاهج نويوكت](#)

[pxGrid ةداهش](#)

[نمآ لال بيولا زاهج لال ع ERS و SXP نويوكت](#)

[فيرعت لال فيرعت فلم](#)

[بيقر لال لال عمئاقولت لال زيمرت لال ك ف ةسايس](#)

[لدبم لال نويوكت](#)

[AAA](#)

[كيسورت](#)

[ةحصل لال نم ققحت لال](#)

[ةلص تاذا تامولعم](#)

عمدقم لال

ISE رشن تايولم عم نم (SGT) نامآ لال عمومجم مقرر تامولعم لال سارا عارج دنتسم لال اذه فصي لال خ نم (WSA) بيولا نامآ زاهج مساب ايمسر فورعم لال (Cisco) نم دحاو نمآ بيو زاهج لال ةددعتم لال TrustSec رشن لال ع SGT لال عمئاقولت لال بيولا لال لوصولت لال تاسايس نم ةدافتسم لال PXgrid.

تاسايس لال ISE نم ةدحاو عمومجم عم لال ةنمآ لال بيولا ةزهجال جمم نكمي ال 14.5 رادصلال لبق لال عافتل نمآ لال بيولا زاهج لال نال نكمي، ديوجل رادصلال اذه لال خدا عم و SGT لال عمئاقولت لال ةيوهال. اهنبي عمجت لال ةلص فنم لال ISE دقع مادختسم لال ISE تاعومجم نم تامولعم لال عم.

فلتختم نم مدختسملا تانايب ري دصت ةينانكم انل حيتي و ةري ب ةدئاف دوعي رمألا اذهو مدختسملل نكمي يتللا جورخلا ةطقن يف مكحتلا ةيروحو (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 وجماربلل تارادصا ىل دنننسملا اذه يف ةدراولا تامولعملل دننست

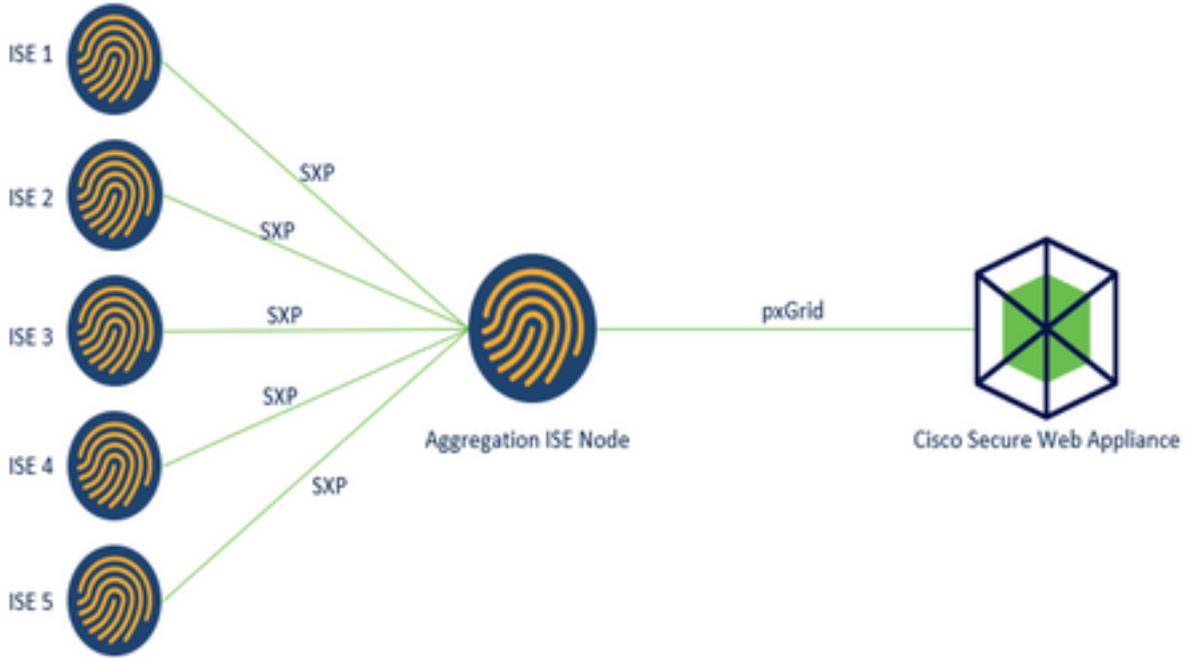
- 14.5 نمألا بيو زاهج
- 3.1 P3 رادصا ل ISE

ةصاخ ةيلمعم ةئيبي يف ةدوجوملا ةزهجالا نم دنننسملا اذه يف ةدراولا تامولعملل ءاشنإ مت تناك اذا. (يضايرتفا) حوسمم نيوكتب دنننسملا اذه يف ةمدختسملا ةزهجالا عيمج تادب رمألا لمحتملا ريثأتلل كمهف نم دكأتف، ليغشتلا ديقتك تكبش

دويقلا

1. ءابقرلل ةدوجوملا تانبيعتلا ىلع ظافحلا ىل ISE تاعومجم عيمج جاتحت.
2. ISE تاعومجم يقابب صاخلا SGTs مقر/مسا ISE عيمجت ةدقعل نوكي نأ بجي.
3. (هيجوتلا/ريفشتللا ك/ف/لوصولا) ةسايسلا ديحت ال نمألا بيو زاهجل نكمي ال مدختسملا مسا الو ةعومجملا ىل الو SGT ةمالع ىل ادانتسا
4. بيقرلا ىلع تامولعملل عبتتو ريراقتلا دادعإ دمتعي.
5. هذه ىلع اهقيبطت يف ةدوجوملا ISE/Secure Web Appliance مچح 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. في لىوختلا
2. SGT- تانىعت لكش في هءه SGT تامولعم لاسراب لك ءءب ءفلءءملا ISE تاعومءم موقت . SXP لالء نم ISE عىمء ءءقعل IP
3. pxGrid رءع ءءاولا نم آلا بىولا زاى عم اهءراشتو تامولعمل هءه ISE عىمء ءءقعل ىقلى ت .
4. ءىناكم ا رىفوتل 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 ءءو ىرسىلا ءىولعل ءىوازلاب ءووم  ءءالءل رطسألا ءنوقى اءء . 1 ءوطءلا رشنلا > ماطنلا > ءءءلا

رىءء قوف رءناواهنىوكء ءىرت ىتلا ءءقعل ءء . 2 ءوطءلا

The screenshot shows the Cisco ISE Administration interface for System. The 'Deployment' tab is active. On the left, there is a navigation pane with 'Deployment' and 'PAN Failover'. The main area is titled 'Deployment Nodes'. At the top right, it says 'Selected 1 Total 1'. Below this, there are buttons for 'Edit', 'Register', 'Syncup', and 'Deregister'. The 'Edit' button is highlighted with a red box. Below the buttons is a table with columns: Hostname, Personas, Role(s), Services, and Node Status. The table contains one row for 'ise01-CL1' with roles 'STANDALONE' and 'SESSION PROFILER'.

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

The screenshot shows the Cisco ISE Administration interface for System. The 'Deployment' tab is active. The main area shows configuration options for 'Enable Session Services'. There are several checkboxes: 'Enable Profiling Service', 'Enable Threat Centric NAC Service', and 'Enable SXP Service'. The 'Enable SXP Service' checkbox is checked and highlighted with a red box. Below it, there is a dropdown menu for 'Use Interface' set to 'GigabitEthernet 0'.

ظفح قوف رقناو لفسألا لفسأل ريرم تلاب مق 4. ةوطخلا

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

ةومجم الما ظن دقع لىل ع SXP نيوكت

لىل ددحو رسيلا ةيولعلا ةيوازلا في دوجوم  ةالثال رطسألا ةنوقيأ ددح 1. ةوطخلا TrustSec > SXP > لمعلا زكرم.

SXP ريطانك ISE عيمجت ةدقع نيوكت ل ةفاضلا+ قوف رقنا 2. ةوطخلا

The screenshot shows the Cisco ISE Administration interface for Work Centers - TrustSec. The 'SXP' tab is active. The main area is titled 'SXP Devices'. At the bottom, there are buttons for 'Refresh', '+ Add', 'Trash', 'Edit', and 'Assign SXP Domain'. The '+ Add' button is highlighted with a red box. There is also a pagination control showing 'Rows/Page 2' and 'Total Rows 2'.

ددح. عم تسمك ريطانلا رود ددحو، ISE عيمجت ةدقع ل IP ناو نعو مسالا في رعتب 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

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 ةوطخل

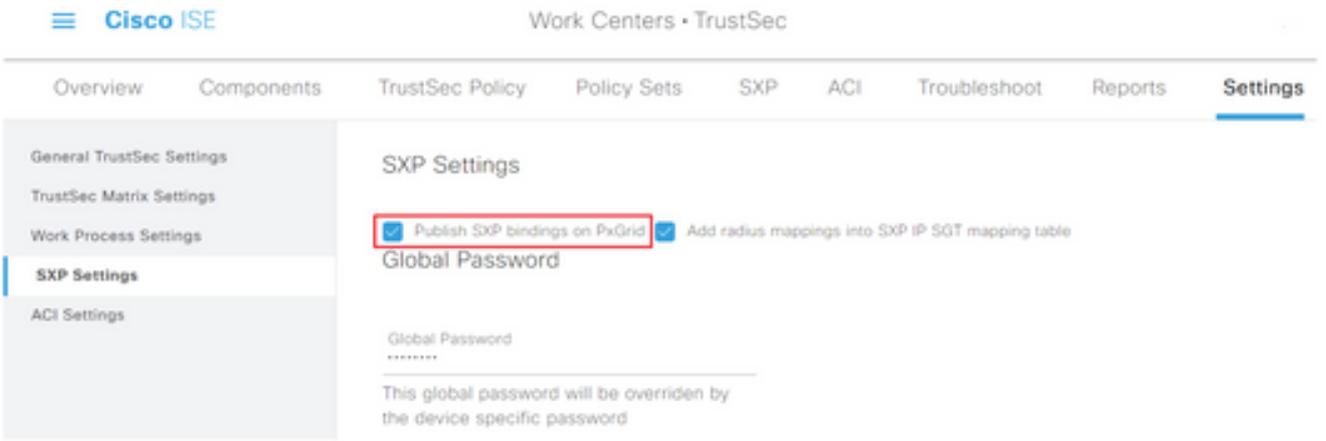
ةدق ب SXP لاصتا ءانبل ةعومجم لك في ISE دق قيا بل تاوطخل اعيمج ررك: ةظحالم ريظن رودك تاوصل ربكم ددحو اعيمجتلا ةدق عل ةلمعل سفن ررك. اعيمجتلا

اعيمجتلا ةدق عل SXP نيوكت

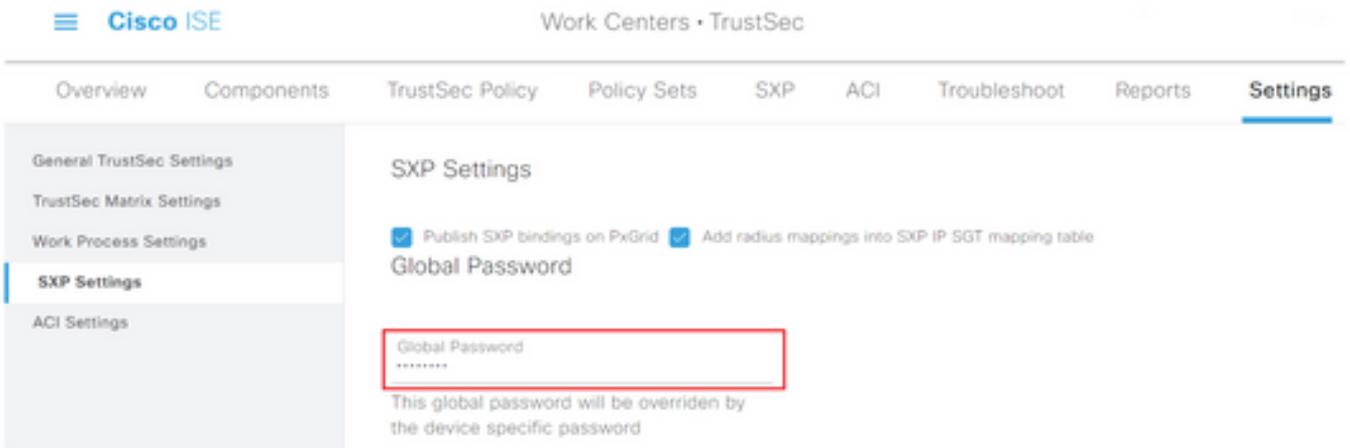
> لمعل زكرم في ددحو رسيالا عل ال نكرلا في ةدوجوم رطسا ةثالث ةنوقيأ ددح. 1 ةوطخل تااداع | TrustSec >

SXP تااداع | ءحفص رقنا. 2 ةوطخل

pxGrid عل SXP طباور رشن رايتخال ءناخ ددح، IP-SGT تاايعيت رشنل. 3 ةوطخل



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

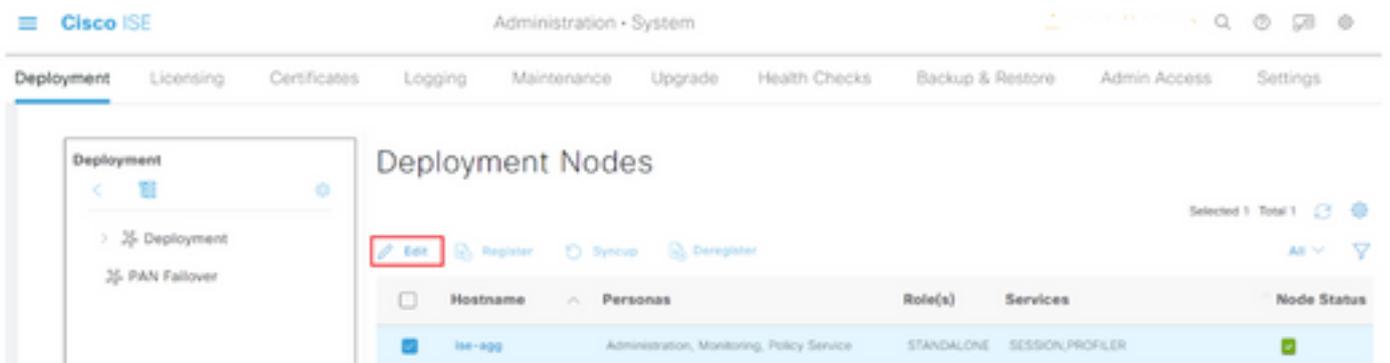


.ظفء قوف رقناو لفسأل ررمرءلاب مق .5 ةوطءلا

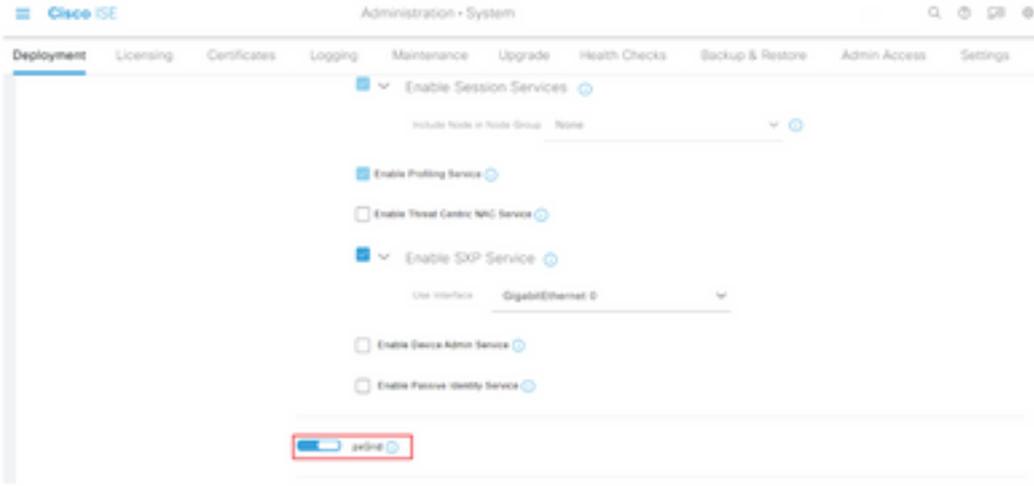
ءءمءءلا ةءقء فف pxGrid نءكمء

ءراءءلا فف ءءو رسءلا ةءولءلا ةءوازلا فف ءءوءوملا ةءالءلا طوءءلا ءنوءفءء ءءء .1 ةوطءلا
> رءنءلا > مءظنءلا >

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



.pxGrid راءءء ءءوءوملا رءلا رقنا، pxGrid نءكمءءلا .3 ةوطءلا

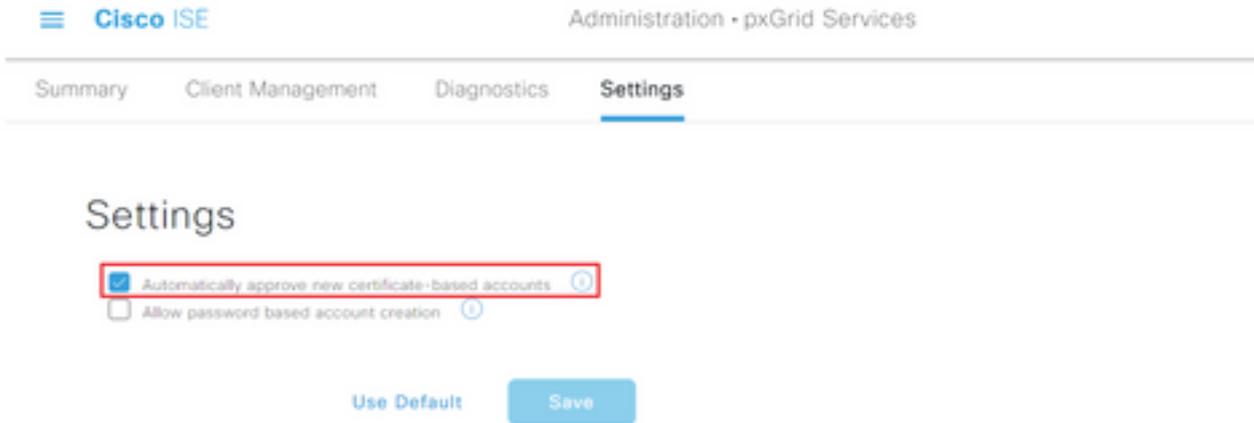


ظفح قوف رقناو لفسألا ىلإ ريرمتلاب مق 4. ةوطخلا

pxGrid ل ىئاقلتلا دامتعالا

> ةرادا ددحو ىرسىلا ةيولعلا ةيوازلا يف ةدوجوم رطسأ ةثالث ةنوقيا ىلإ لقتنا 1. ةوطخلا
تادادعا > pxGrid تامدخ

pxgrid ءالمع نم pxGrid لاصتاتابلط ىلع ىئاقلتلا ISE قفاوي ال ،اىضارتفا 2. ةوطخلا
ىلع ةيئاقلتلا ةقفاوملا رايئتخالا ةناخ ديدحت قيرط نع دادعإلا اذه نيكمت بجي كلذل ،ددجلا
ةداهش ىلإ ةدنتسمل ةديدل تابلطال



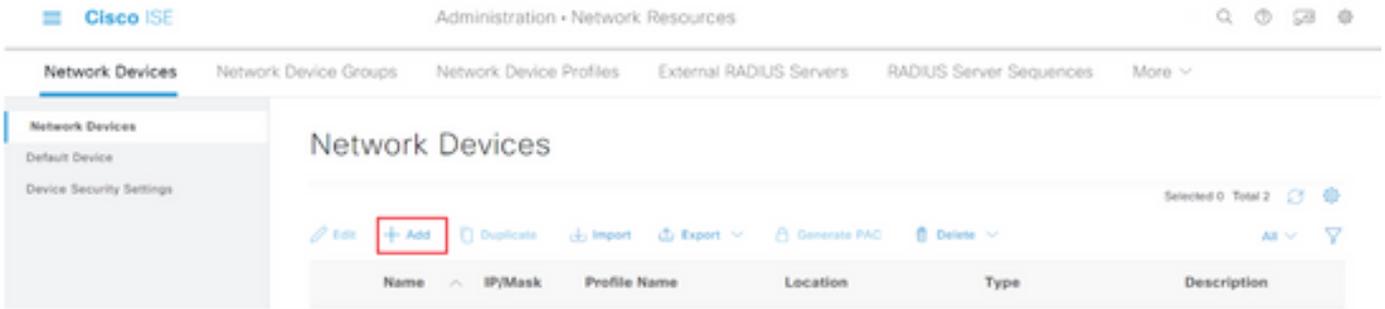
ظفح ةقطق 3. ةوطخلا

ةكبشلا ةزهجال TrustSec تادادعا

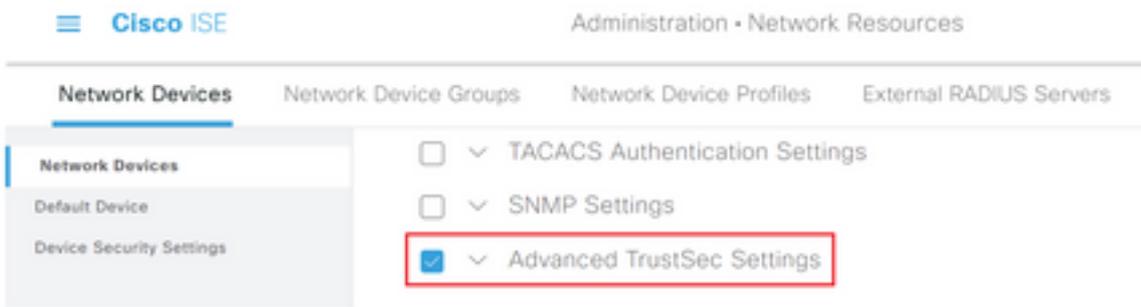
بجي ،اهىلع TrustSec نيكمت مت ىتلا ةزهجال نم تابلطالا ةجلاعم نم Cisco ISE نكمتي يكل
Cisco ISE يف اهىلع TrustSec نيكمت مت ىتلا ةزهجال ديدحت كىلع

> ةرادا ىلع ددحو رسيالا يولعلا نكرلا يف ةدوجوملا ةثالثلا طوطخلا ىلإ لقتنا 1. ةوطخلا
ةكبشلا ةزهجا > ةكبشلا دراوم

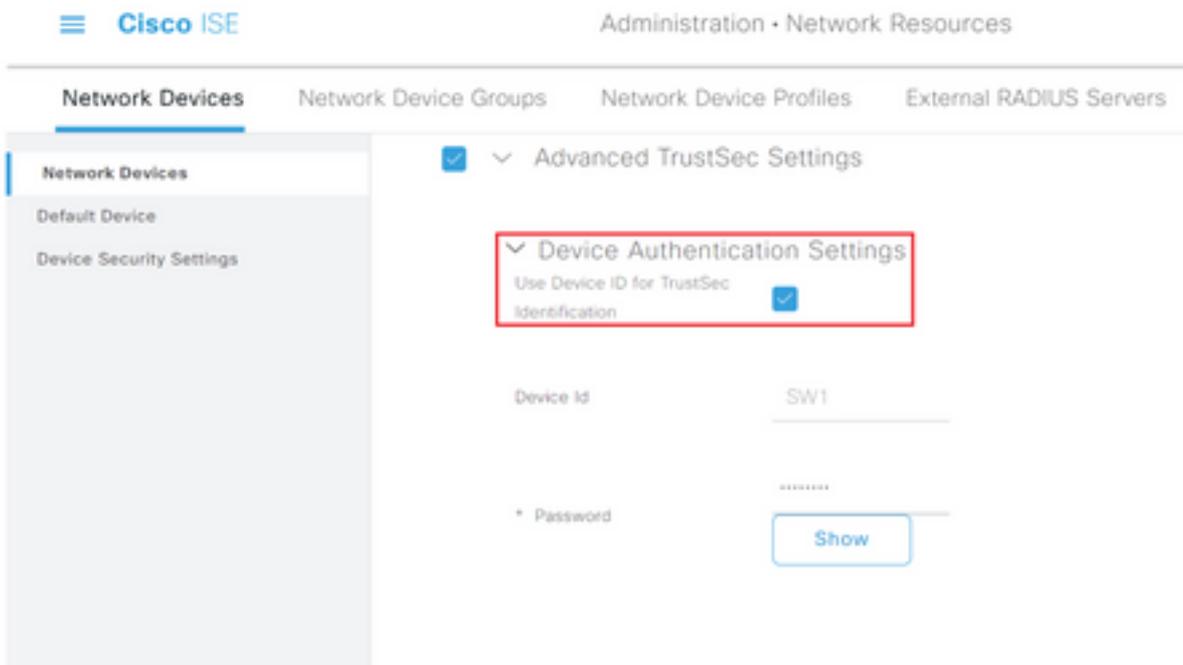
ةفاضلا+ ةقطق 2. ةوطخلا



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

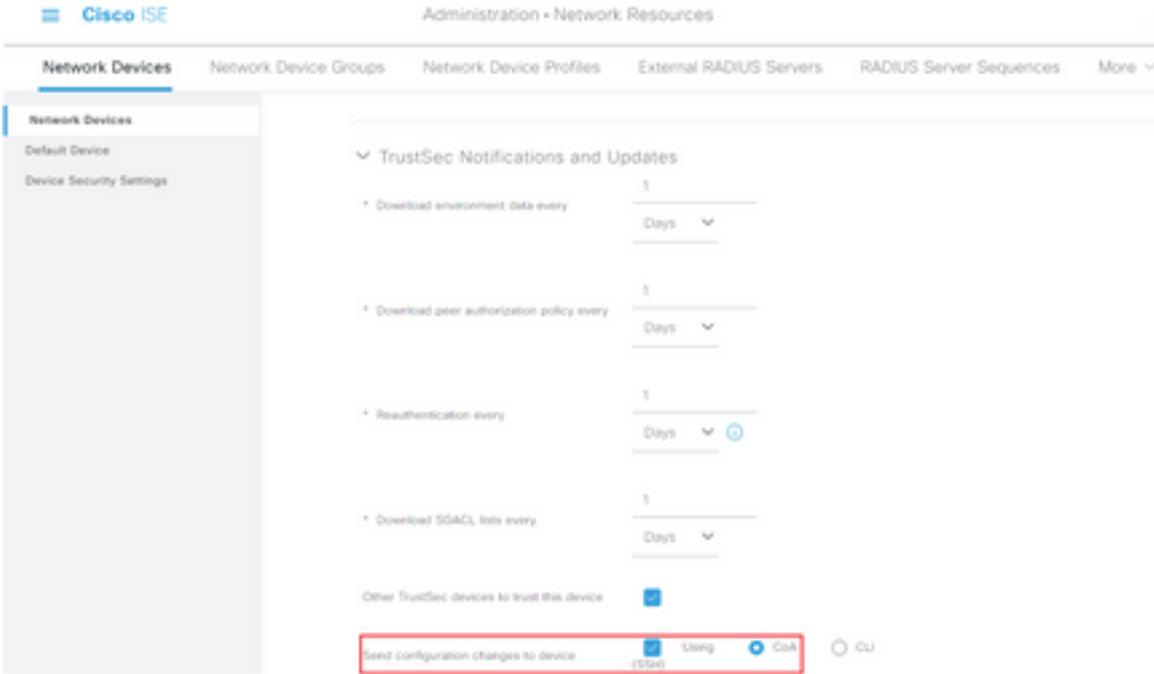


مسا ميمعتل TrustSec فيرعتل زاهجل فرعم مادختسا رايتخاله ةناخ يلع رقنا. 5 ةوطخل
رورملا ةملك ل قح يف رورم ةملك لخدأ. ايايقلت ةكبشلا ةزهجأ مسق يف دورسلا زاهجل



مظالم "cts credentials id <id> password
لوحمل يلع اقحاله نيوكت مت يذلا <pw>".

لاسرنا نم ISE نكم تي شيح زاهجل ل نيوكتل تاريخيغت لاسرا رايتخاله ةناخ ددح. 6 ةوطخل
زاهجل يل TrustSec نم CoA تامالعه



نام ألة وعمجم عمال ع نبيعت تاثير دحت رشن دنع زاهجال اذه نيمضت راي تخال اة ناخ ددح . 7 ةوطخال

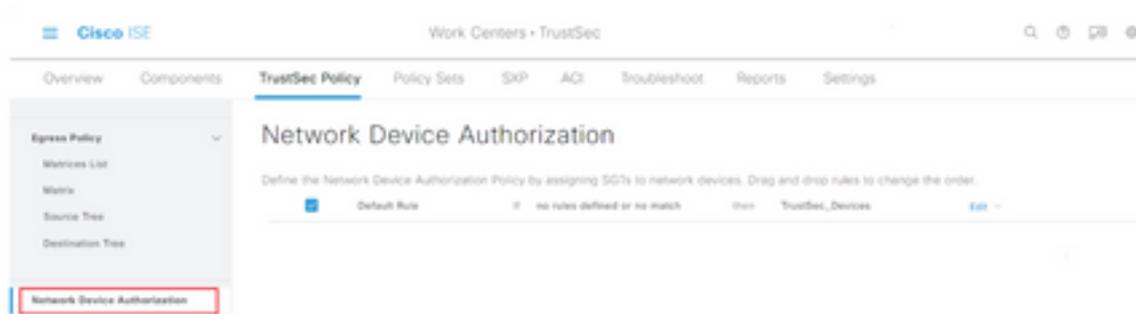
تاغوسم لمعتسم لال ، اءا ءك بشل نم لئك شتل ل ررررر ISE تكترت in order to تلخد . 8 ةوطخال
 لال ف ءم لك enable ، رراي تخال ءوزي . لال عم لك بولس EXEC و username بولس EXEC لال ف
 لال عم لك بولس enable .

TrustSec لال عم نم اعز نوك نأ دصقي يتل ال رخال ال NADs عي عم ل تاوطخال ررك : ءطخال

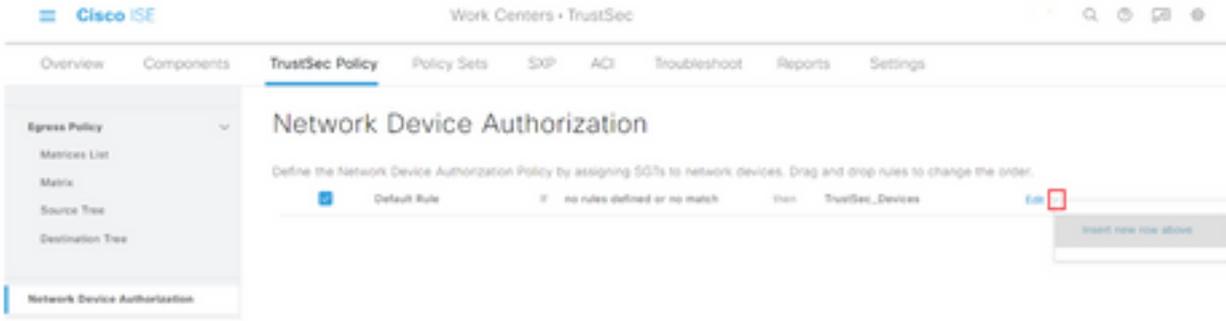
ءك بشل زاه ضي وفت

زكارم ي ف ددحو رسي لال ءيول لال ءي وازل ي ف ءدو و م لال ءال لال طوطخال ءنوقي ي ددح . 1 ةوطخال
 لال عم لك بولس enable > TrustSec > هن

ءك بشل زاه ضي وفت لال ع رقال ، رسي ال اعزل ي ف . 2 ةوطخال

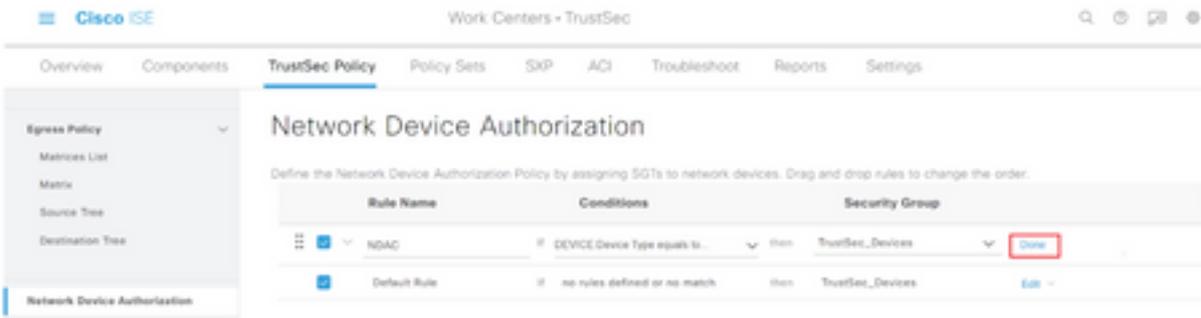


الاع ءي ء ف ص ءارءاو ررررر لال ءروا عم ال ءلءس نم ال ءمءال لال مءءسأ ، نيمي لال لال ع . 3 ةوطخال
 ءي ء NDA ءءاق ءاشن ال



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

نيميللا يصقأ لىا مت ةقطق 5. ةوطخلا



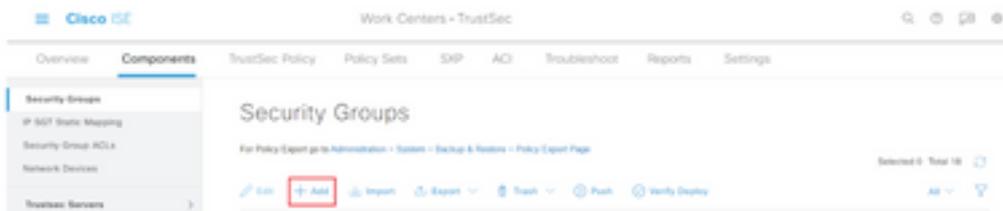
ظفح قوف رقناو لفسأل ريرمتلاب مق 6. ةوطخلا

بيقر

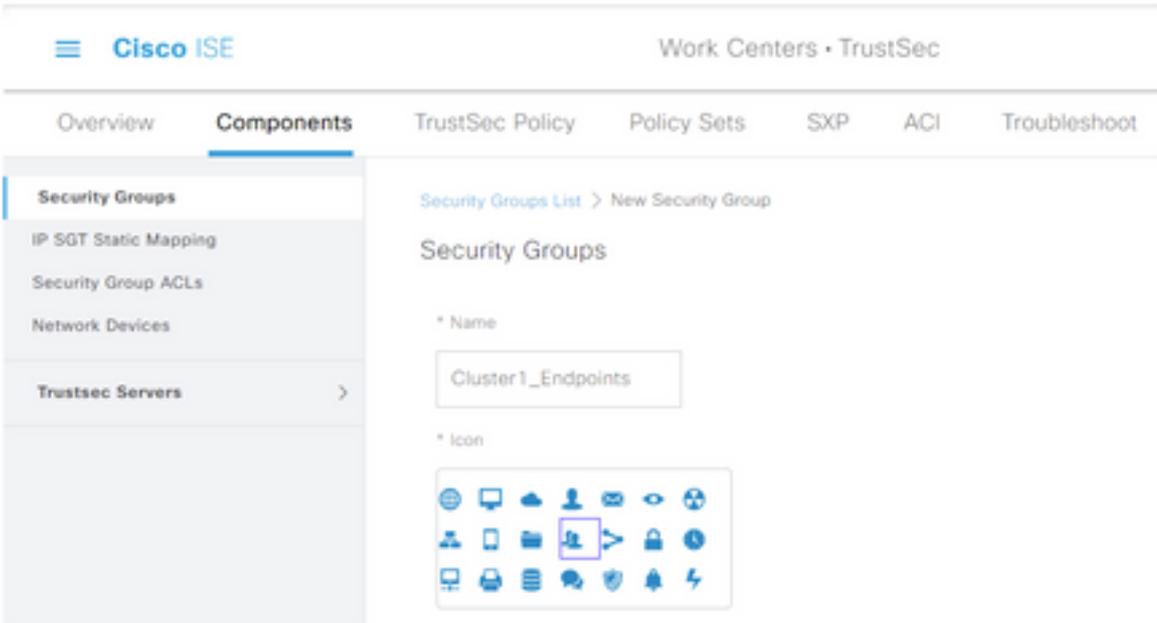
زكارم يف دحو ورسيلع ال نكرلا يف ةدوجوملا ةثالثلا طوطخلا ةنوقيأ دحو 1. ةوطخلا تانوكملا > TrustSec > لمعلا

نامالا تاعومجم عيسوتب مق ،رسيالا عزجال يف 2. ةوطخلا

ديدج بيقر عاشنال ةفاضلا+ رقنا 3. ةوطخلا



ةبسانملا لوقحلا يف ةنوقيأ رتخاو مسالا لخدأ 4. ةوطخلا



زېږېمت ؤمالع ؤمېق لخدأو افسو هطعأ ،ايرايختا. 5 ؤوطخلا

> لمعال زكارم لىل لوقتنا ،اىوډي زېږېمت ؤمالع ؤمېق لخدأو نم نكمتلا لجا نم :عظالم
مقرر لخدأو مدختسم لىل عېجې رايخلا ددحو General TrustSec تاداع | > تاداع | TrustSec >
ناملال ؤومجم ؤمالع مېقرت تحت اىوډي بېقرلا

لاسرا قوف رقناو لفسأل ريرمتلاب مق. 6 ؤوطخلا

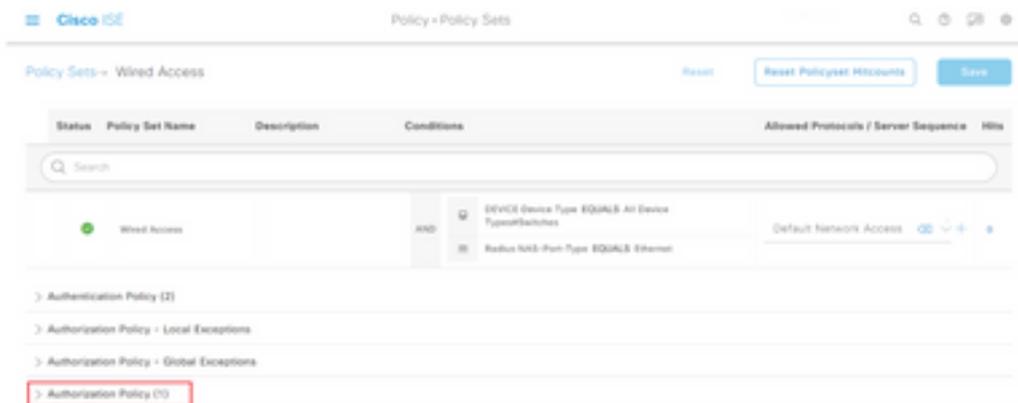
نېبولطم لىل عابقرلا عېمجل تاوطلالا هذو ررك :عظالم

لېوختلا ؤسايس

ي ف ددحو ىرسىللا ؤيولعللا ؤيوازلا ي ف ؤدووملا ؤثالثلا طوطخلا ؤنوقى ددح. 1 ؤوطخلا
تاسايسلا تاعومجم > ؤسايسلا

ةبسانملا جهنلا ؤومجم ددح. 2 ؤوطخلا

لېوختلا جهن عيسوتب مق ،جهنلا ؤومجم نمض. 3 ؤوطخلا



لېوخت چهن عاشن رز قوف رونا 4. ؤوخل



Authorization Policy (1)						
Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Actions

بېقرلا ددو ؤبولطم ال فيرعتل تا فلوم و s/طرشل او ؤءاقل مسا دي دحت ب مق 5. ؤوخل نام ال تا ؤومجم تحت ؤلدسننم ال ؤمءاقل نم بسانم ال

Authorization Policy (1)						
Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
	Delta-Policy	wwws_802.1x	PermitAccess	Cluster1_Endpoints		

ظفح ؤقطط 6. ؤوخل

ي راي خا ISE ؤمي جت ال ؤقق ي ل ع ERS ني كمت

اهن ع مالعتسال نكمي (API) تاقي بطت ؤجرب ؤه او يه (ERS) ؤي ج راخ ال RESTfull API ؤمدخ ي ضار ت فا لك شب ERS ؤمدخ لي طعت متي. ؤ ؤومجم ال تامول عم ي ل ع ل و ص ح ل ل WSA ؤط ساوب اذ ا (API) تاقي بطت ال ؤجرب ؤه او نع مالعتسال ال مال عمل نكمي، اهن ني كمت درجم بو. ISE ي ل ع ؤفاضا و ISE ي ل ع ؤمدخ ال ني كمت ل. ISE ؤقق ي ل ع ERS لوؤسم ؤ ؤومجم ؤاضع ا ؤقدا صمب اوم اق ؤي ل ال تا و ط خ ال ع بتا، ؤحي ح ص ل ؤ ؤومجم ال ي ل با س ح:

> ؤرا د ي ل ع ددو ي رسي ل ؤي و ل ع ال ؤي و ا ز ل ي ف ؤدو ج و م ال ؤا ل ث ال ط و ط خ ال ؤن و ق ي ا دد ح 1. ؤوخل تا د ا د ع ال > ما ظن ال

ERS تا د ا د ع ي ل ع رونا، ي رسي ل ؤحول ال ي ف 2. ؤوخل

ءبا ت ك ل / ؤءا ر ق ل ل ERS ني كمت راي خ ال دد ح 3. ؤوخل

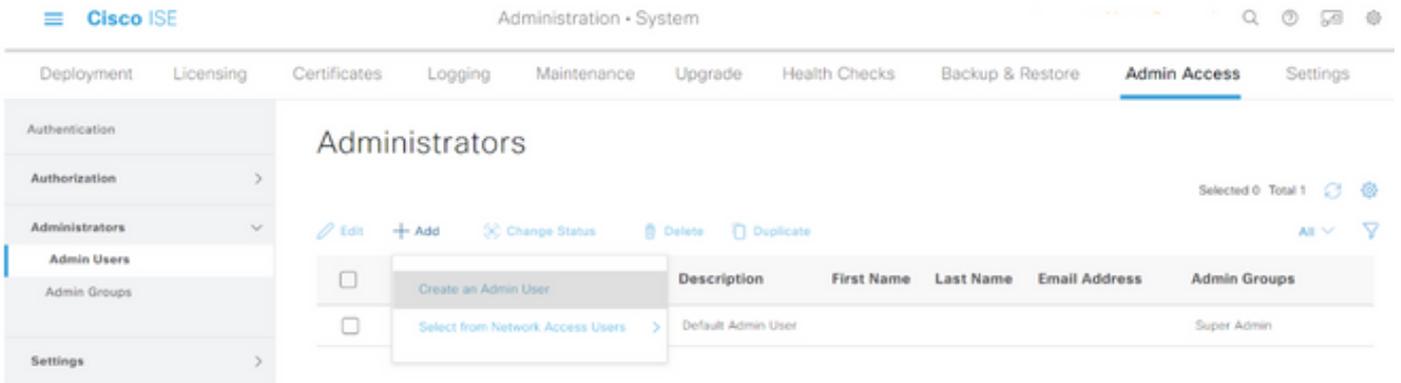
OK. م ادختساب ديكأتو ظفح قوف رقنا 4. ةوطخلا

(يراي تخ) ESR ةرادا ةومجم لىل مدختسم ةفاضل

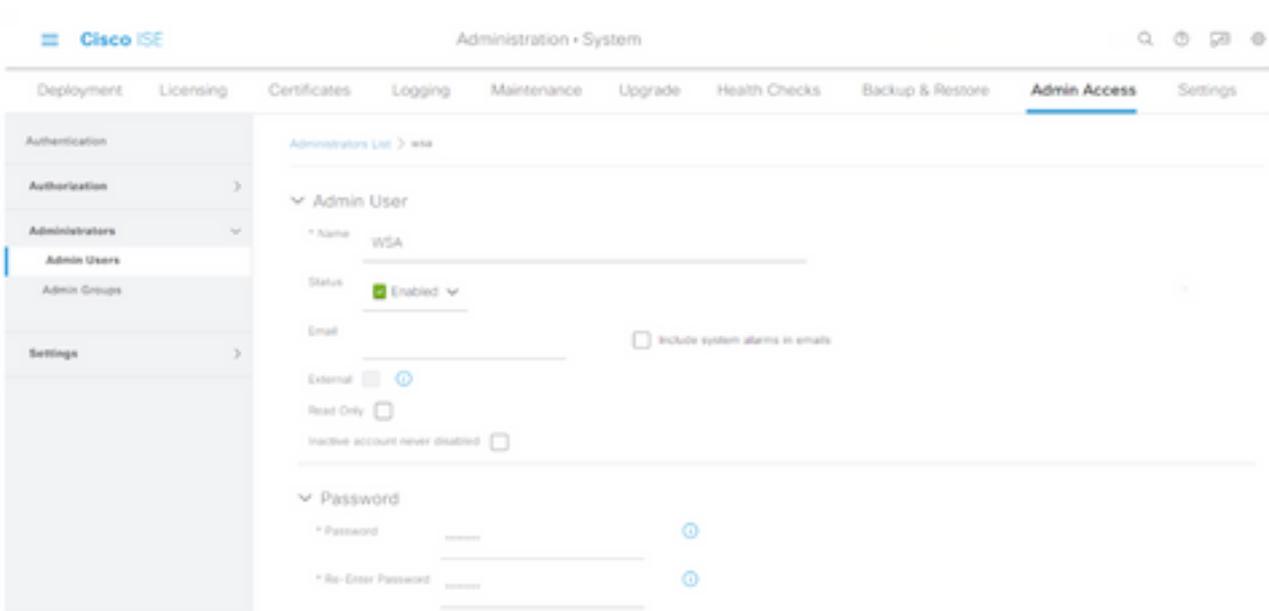
> ةرادا ددحو ىرسىلا ةيولعل ةيوازلا يف ةدوجوملا ةثالثلا رطسألا ةنوقىأ ددح 1. ةوطخلا
لوؤسملا لوصو > ماظن

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

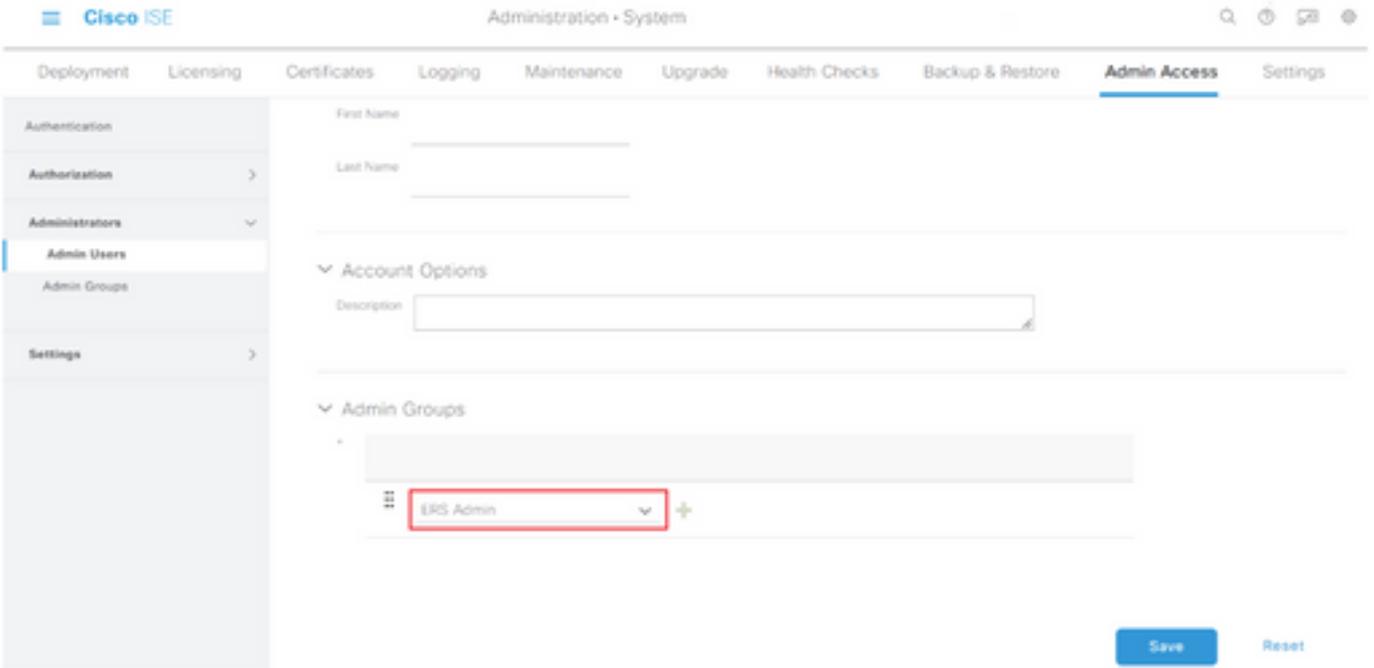
ةلدسنملا ةمئاقلا نم لوؤسملا مدختسم ددحو ةفاضل+ قوف رقنا 3. ةوطخلا



ةبسانملا لوقحلا يف رورم ةمك و مدختسم مسال خذا 4. ةوطخلا



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



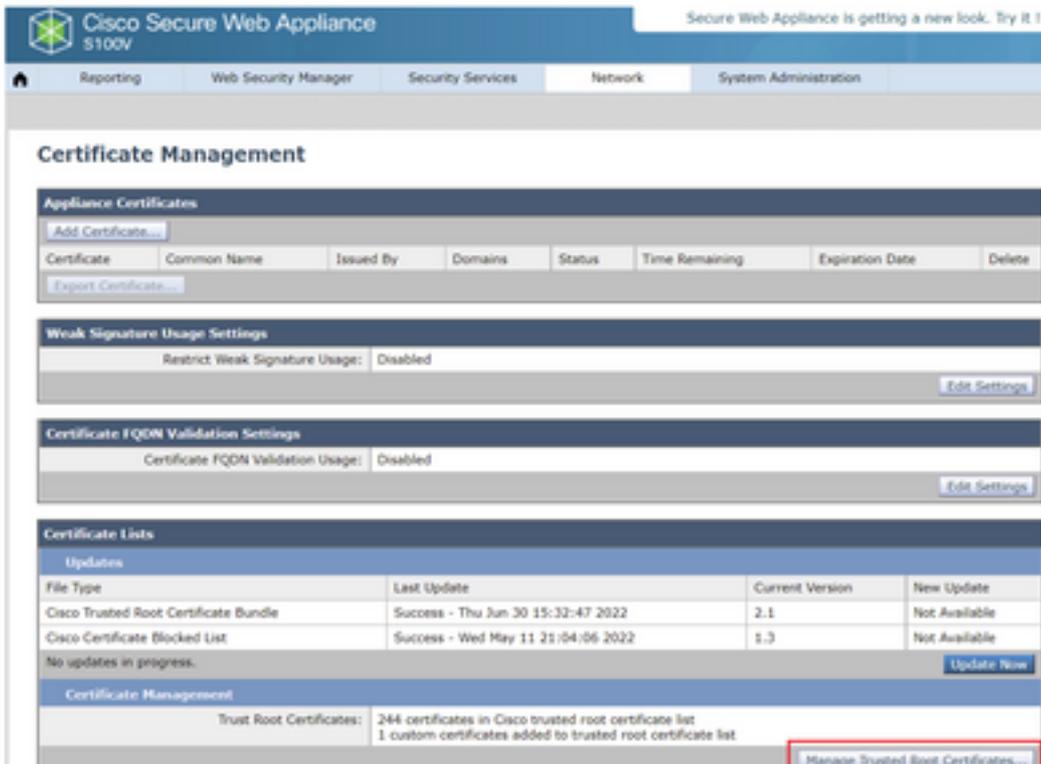
طفا ع ققط ط. 6 ؤوطالا

نمآلا بوللا زاغ نلوكا

رذال ؤءاهشلا

ISE و WSA نل ب لاصا ل ؤقلا ل رذال ل ؤءاهش عرجم مءءسا سلا لماءا ل ملام صا نا اءا نل زاغال الك ل ع هءه رذال ؤءاهش ءل بءء باءل.

ءب قوءوملا رذال ؤءاهش ؤراءا ل ع رقا و ؤءاهشلا ؤراءا > ؤءبشلا ل لقا نا. 1 ؤوطالا ؤقا قءصم عرجم ؤءاهش ؤاضالا



داري تس | قوف رونا 2. ةوطخل



رقناو هؤاشن | مت يذلا رذجال قدصم ل عجرم ل عقوم ديحت ل فلم رايخ | قوف رونا 3. ةوطخل لاسرا قوف

ىرخأ ةرم لاسرا قوف رونا 4. ةوطخل

تاريغت ل ديكتأ رونا، ىنم يلا ةيولعل ةيوازلا ي 5. ةوطخل



ىرخأ ةرم تاريغت ل ذيفنت قوف رونا 6. ةوطخل

pxGrid ةداهش

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

ةيول ةمدخ كرحم > ةكبش ل ل ل ل قنتا 1. ةوطخل

تادادع ل ريرحت و نيكت ىل ع رونا 2. ةوطخل

رقناو هؤاشن | مت يذلا رذجال قدصم ل عجرم ل عقوم ديحت ل فلم رايخ | قوف رونا 3. ةوطخل فلم ل ليحت قوف



بجي .مسق ل اذه ي pxGrid ISE ةداهش ل ليحت وهو ءاش نيوكت أطخ كانه :ةطخال
pxGrid ISE ةدق ةداهش ل قح ىل رذجال قدصم ل عجرم ل ةداهش ل ليحت

مت نيذلل حاتفم ل او ةداهش ل مادختس | دح، بيولا زاه ل لي مع ةداهش مسق ي 4. ةوطخل
امه ءاشن |

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 لمك أو 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 لاسرإ رزلا ديدجت نسحتسملا م :ةظحالم يتلا ةداهشلا وحياتافملا دوقف نكمي ،تاريخي غتلا لاسرإ 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: ws-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 ي ت ل م دخت س م ل تام ول عم ل خ دأ ، ERS لوؤسم تاغ وسم ل ق ح ي ف 2 ةوطخ ل ISE.

م ي ت ل م تام ول عم ل ثرت ل ISE pxGrid ةدق ع ل هس فن م داخ ل م س ا ل ع ب ر م ل د د ح 3 ةوطخ ل . كانه ةبول ط م ل تام ول عم ل ل خ د ا ف ، ا ل و . ا ق 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

ف ي ر ع ت ل ف ي ر ع ت فلم

فلم عاشن إ ب جي، WSA تاسايس في ISE ةومجم تامولعم وأ نامألة ةومجم تامالع مادختسال ةيفافش ب نيمدختسملل فيرعتلة لسيوك ISE مدختسي فيرعت

فيرعتلة تافيصوت > ةقداصملا > بيولا نامأ ريدم لة لقتنا. 1 ةوطخل

فيرعت فيصوت ةفاضل لة رقتنا. 2 ةوطخل

ايرايخا فصوو امسا لخدأ. 3 ةوطخل

فيرعت رايخال ةلدسنملا ةمئاقلا مدختسأ، ةقداصملا و فيرعتللا مسق في. 4 ةوطخل ISE مادختساب ةيفافش ب نيمدختسملل

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:	2 (Global Profile)

User Identification Method	
Identification and Authentication:	Transparently identify users with ISE
Fallback to Authentication Realm or Guest Privileges:	If user information is not available from the Identity Services Engine: <input type="text" value="Support Guest Privileges"/> <small>Authorization of specific users and groups is defined in subsequent policy layers (see Web Security Manager > Decryption Policies, Routing Policies and Access Policies).</small>

Membership Definition	
Membership is defined by any combination of the following options. All criteria must be met for the policy to take effect.	
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
Advanced Define additional group membership criteria.	

مازتلاو لاسرا. 5 ةوطخل

بيقرلا لة ةمئاقلا زيمرتلا ك ةسايس

ريرفتللا ك ةسايس > بيولا تاسايس > بيولا نامأ ةرادا لة لقتنا. 1 ةوطخل

جهن ةفاضل قوف رقتنا. 2 ةوطخل

ايرايخا فصوو امسا لخدأ. 3 ةوطخل

ةلدسنملا ةمئاقلا مدختسأ، نيمدختسملل و فيرعتللا تافيصوت مسق في. 4 ةوطخل رثكأ و دحاو فيرعت فيصوت ديدحت رايخال

فلم مسا رايخال ةلدسنملا ةمئاقلا مدختسأ، فيرعتللا تافيصوت مسق في. 5 ةوطخل ISE فيرعت

ةددحملا تاعومجملا ددح، ةدمتعمللا تاعومجملا و نومدختسمللا مسق في. 6 ةوطخل نيمدختسمللا و

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 ةومجملا 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 بيقرلا ةمهم

ةقداصملا حاجن دعب اهل بيقرن نييعت مت 1 ISE ةومجم نم ةياهن ةطقن ةيؤر انه كنكمي
ضيوفتلاو:

Time	Identity	Endpoint ID	Endpoint Profile	Authentication Policy	Authorization Policy	Authorization Profile	IP Address	Security Group	Server
Jan 14, 2023 12:07:46 AM	Admin@sw01	14.50.50.1	IP Default	Sw01 Access --> S...	Sw01 Access --> S...	PermitAccess	10.50.50.12	Cluster1_Endpoint	ise01-cl1

ةقداصملا حاجن دعب اهل بيقرن نييعت مت 2 ISE ةومجم نم ةياهن ةطقن ةيؤر انه كنكمي
ضيوفتلاو:

Time	Identity	Endpoint ID	Endpoint Profile	Authentication Policy	Authorization Policy	Authorization Profile	IP Address	Security Group	Server
Jan 14, 2023 03:08:47 PM	Admin@sw01	14.50.50.1	Microsoft Work	Sw01 Access --> S...	Sw01 Access --> S...	PermitAccess	10.50.50.12	Cluster2_Endpoint	ise01-cl1

SXP تانبييعت

فرعتلال متي، ISE عيمجت ةدقعو ةومجملا ماظنل ISE دقع نبي SXP لاصتلا نيكم تل ارظنو
SXP لالخن نم ISE عيمجت ةطساوب هذه SGT-IP تانبييعت 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 إلى، فلتختم ال ISE اوعومجم نم، هذه SXP تانيي عت لاسرا لك لذ دع ب متي ISE عي مجت ةدق ع لال خ

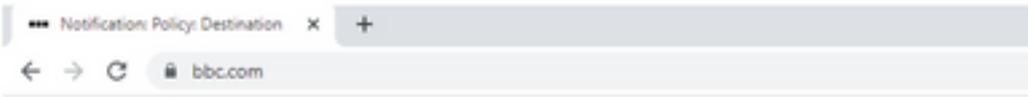
```
wsa2.securitylab.net> isedata
Choose the operation you want to perform:
- STATISTICS - Show the ISE server status and ISE statistics.
- CACHE - Show the ISE cache or check an IP address.
- SGTs - Show the ISE Secure Group Tag (SGT) table.
- GROUPS - Show the ISE Groups table.
[>] cache

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   -
```

بي قيرلا إلى ع مئاقلا تاسايسلا قي بطت

امك، اهب ةصاخلا تاسايسلا عم قباطت يتلا ةفلتختم ال ةياهنلا طاقن ىرت نأ انه كنكمي اهلجريس إلى ادانتسا رورملا ةكح عنم متي

ISE 1 ةوعومجم إلى يمتنت يتلا ةياهنلا ةطقن



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
04 Jul 2022 14:28:17	https://bbc.com/443/television CONTENT TYPE: - URL CATEGORY: Block URLs CL1 DESTINATION IP: DETAILS: Decryption Policy: 'ISE_Cluster1', WBARs: 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 ةي وهلا ةمدخو بي وهلا نامأ زاها لم اكاك لىل](#)
- [TrustSec تامدخ ل ISE عم WSA لم اكاك نيوكا](#)
- [Cisco، نم ةي وهلا تامدخ كرحم لوؤسم لىل](#)
- [Cisco Secure Web Appliance ل AsyncOS 14.5 ل مدختس مل لىل](#)

ةمچرتل هذه لوج

ةللأل تاي نقتل نمة ومة مادختساب دن تسمل اذة Cisco تمةرت
ملاعلاء انء مء مء ف 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 لاعل او
ىل إأمءءاد ءوچرلاب ةصوء و تامةرتل هذه ةقء نء اهءل وئس م Cisco
Systems (رفوتم طبارل) ةلصلأل ةزءل ءن إل دن تسمل