

FMC ربع FTD ىل ع لىجستلا نيوكت

تايوت حمللا

[قم دق م ل ا](#)

[ق ي س اس ا ل ا ت ا ب ل ط ت م ل ا](#)

[ت ا ب ل ط ت م ل ا](#)

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

[ق ي س اس ا ت ا م و ل ع م](#)

[ن ي و ك ت ل ا](#)

[م ا ع ل ل a syslog ن ي و ك ت ن ي و ك ت](#)

[ل ي ج س ت ل ا د ا د ع ا](#)

[ت ا د خ ا ل ا م ي ا و ق](#)

[ل د ع م ل ا د ي ج ت Syslog](#)

[ت ا د ا د ع ا Syslog](#)

[ي ل ج م ل ل ا ل ي ج س ت ل ا ن ي و ك ت](#)

[ي ج ر ا خ ل ل ا ل ي ج س ت ل ا ن ي و ك ت](#)

[د ع ب ن ع Syslog م د ا خ](#)

[ل ي ج س ت ل ل ي ن و ر ت ك ل ل ا ل ا د ي ر ب ل ا د ا د ع ا](#)

[ق ح ص ل ل ا ن م ق ق ح ت ل ا](#)

[ا ه ح ا ل ص ا و ا ط ا خ ا ل ا ف ا ش ك ت س ا](#)

[ق ل ص ت ا ذ ت ا م و ل ع م](#)

ق م د ق م ل ا

J- FirePOWER Threat Defense (FTD) J- Firepower Management Center (FMC) ل و خ د ل ا ل ي ج س ت ن ي و ك ت د ن ت س م ل ا ا ذ ه ف ص ي

ق ي س اس ا ل ا ت ا ب ل ط ت م ل ا

ت ا ب ل ط ت م ل ا

ق ي ل ل ا ت ل ا ع ي ض ا و م ل ا ب ق م ك ي د ل ن و ك ت ن ا ب Cisco ي ص و ت:

- FirePOWER ق ي ن ق ت
- (ASA) ق ل د ع م ل ا ن ا م ا ل ا ق ز ه ج ا
- Syslog ل و ك و ت و ر ب

ق م د خ ت س م ل ا ت ا ن و ك م ل ا

ق ي ل ل ا ت ل ا ق ي د ا م ل ا ت ا ن و ك م ل ا و ج م ا ر ب ل ا ت ا ر ا د ص ا ل ا د ن ت س م ل ا ا ذ ه ي ف ق د ر ا و ل ا ت ا م و ل ع م ل ا د ن ت س ت

- ASA Firepower ل ASA (5506X/5506H-X/5506W-X، ASA 5508-X، ASA 5516-X) ت ا ر ا د ص ا ل ا و 6.0.1 ج م ا ن ر ب ل ا ر ا د ص ا ب ل م ع ت ي ت ل ا

- شذألأ تارادصلإل او جم ان ربلأ نم 6.0.1 رادصلإل لغشت يتلأ (ASA 5515-X، ASA 5525-X، ASA 5545-X، ASA 5555-X، ASA 5585-X) عافدلأ ةروص
- شذألأ تارادصلإل او 6.0.1 رادصلإل FMC

ةصاخ ةيلمعم ةئيب يف ةدوجوملأ ةزهجالأ نم دنتسملأ اذف ةدراولأ تامولعملأ ءاشنإ م تناك اذأ. (يفضارتفا) حوسمم نيوكتب دنتسملأ اذف يف ةمدختسملأ ةزهجالأ عيمج تآدب رمأ يأل لمحتحملأ ريثأتلل كمهف نم دكأتف ،لغشتلأ ديق كتكبش

ةيساسأ تامولعم

هئاطخأ فاشكتساو FTD زاهج ةبقارمل ةمزالل تامولعملأ FTD ماظن تالچس كل رفوت اهحالصاو.

ثداوچلأ ةچلعم يفو يفني تور لكشب اهحالصاو ءاطخألأ فاشكتسا يف ةديفم تالچسلأ دعت ءاوس دح ىلع يچراخلل او يلحملل ليچستلأ FTD زاهج معدف. ءاوس دح ىلع

يچراخلل ليچستلأ. اهحالصاو live ءاطخأ فاشكتسا ىلع يلحملل ليچستلأ كدعاسي نأ نكمي يچراخ syslog مداخلل FTD زاهج نم تالچسلأ عمجل ةقيرط وه

دعاسي نأ نكمي. تاهي بنتلأو تالچسلأ عيمجت يف يزكرم مداخلل ليچستلأ دعاسي ثداوچلأ ةچلعمو لچسلأ طابترا يف يچراخلل ليچستلأ

يلخادلأ تقؤملا نزخملأو مكحتلأ ةدحو رايف FTD زاهج معدف ،يلحملل ليچستلأ ةبسنلاب Secure Shell (SSH) لعم ةسلج ليچستو

ديربلل ليحرت مداخلو يچراخلل syslog مداخل FTD زاهج معدف ،يچراخلل ليچستلأ ةبسنلاب يينورتكللال.

 ديدحت/ليچستلأ عون ىللإ هبتنا ،زاهجلأ ربع ةريبك رورم ةكرح ترم اذأ: ءظحالما رادج ىلع ريثأتلأ بنجتف يذلأو ،تالچسلأ ددع ديدحتل ءارجلأ اذهب مق. لدملأ/ةروطخلأ ةيامحلأ.

نيوكتلأ

ةمالع Platform Settings ىللإ لاقتنالأ دنع ليچستلأ ةقلعتملأ تانويوكتلأ عيمج نويوكت نكمي ةروصلأ هذف يف حضوم وه امك Devices > Platform Settings رتخأ. بويوكتلأ ةمالع Devices لفسأ بويوكتلأ

Overview	Analysis	Policies	Devices	Objects	AMP
Device Management	NAT	VPN	Platform Settings		

ءاشنإل Threat Defense Settings رتخأ م، New Policy رقت نأ وأ ةدوجوملأ ةسايسلأ ريرحتل صاصرلأ ملقلا ةنوقيأ رقت نأ اما ةروصلأ هذف يف حضوم وه امك ةديج FTD ةسايس.

Platform Settings	Device Type	Status	New Policy
FTD-Policy	Threat Defense	Targeting 1 devices Up-to-date on all targeted devices	Firepower Settings Threat Defense Settings

ةروصولا هذه يف حضورم وه امك Save رقناووجهنلا اذه قيبتل فTD زاخ رتخأ

New Policy

Name:

Description:

Targeted Devices

Select devices to which you want to apply this policy.

Available Devices

Search by name or value

- FTD_HA

Selected Devices

- FTD_HA

ماعال syslog نيون نيونكت

ةمزالالا تاملعمل عم مسقلا اذه لماعتي .يخراخالاوليحمل ليجستلا نم لك ىلع قيبتلل ةلباق ةنيعم تانيونكت كانه syslog. لاهنيونكت نكمي يتلا ةيرايتخالاول

ليجستلا دادع

Devices > رتخأ ،ليجستلا دادع نيونكتل .يخراخالاوليحمل ليجستلا ىلع قيبتلل ةلباق ليجستلا دادع |تارايخ نوكت **Platform Settings.**

رتخأ . Syslog > Logging Setup

يساسال ليجستلا دادع

- **Enable Logging:** ددح **Enable Logging** ةناخ ددح. ليجسستلا نيكمتل رايختالال.
- **Enable Logging on the failover standby unit:** ددح **Enable Logging on the failover standby unit** ةناخ ددح. نيكمتل رايختالال. رفاوتلا ةلعال FTD ةومجم نم اعزج دعي ذللا يطايتحالال FTD لىل لوخدلا ليجست.
- **Send syslog in EMBLEM format:** ددح **Send syslog in EMBLEM format** ةناخ ددح. راعشك syslog قيسنت نيكمتل رايختالال. اذه قفاوتي. CiscoWorks (RME) دراوم ةرادال Syslog لىل حمل سيسيئر لكشب راعشلا قيسنت مادختسا متي. ةهجو لك لطق رفاوتي. تالوحو لاولا ةطساوب هجاتن مت ذللا Cisco IOS Software جمانربل Syslog قيسنت عم قيسنتالال UDP syslog مداوخل.
- **Send debug messages as syslogs:** ددح **Send debug messages as syslogs** ةناخ ددح. اعطالال حيحصت تالجس لاسرال رايختالال Syslog مداخل لىل Syslog لىل سرك.
- **Memory size of the Internal Buffer:** ددح **Memory size of the Internal Buffer** ةناخ ددح. لىل فلد نيكمتل رايختالال. تاقوملا ةركاذلا نزم مجح لخدأ. تاقوملا نزم لىل لوصول مت اذال لىل فلد تانايب ريودت متي.

(يرايختالال) FTP مداخل تامولعم

يلخدالال تاقوملا نزم لىل لادبتساوب موقت نأ لبق FTP مداخل لىل لىل فلد تانايب لاسرال ديرت تنك اذال FTP مداخل لىل صافات ددح.

- **FTP Server Buffer Wrap:** ددح **FTP Server Buffer Wrap** ةناخ ددح. لىل فلد نزم لىل لىل فلد تانايب لاسرال رايختالال.
- **IP Address:** ددح **IP Address** ةناخ ددح. لىل فلد نزم لىل لىل فلد تانايب لاسرال رايختالال.
- **Username:** ددح **Username** ةناخ ددح. لىل فلد نزم لىل لىل فلد تانايب لاسرال رايختالال.
- **Path:** ددح **Path** ةناخ ددح. لىل فلد نزم لىل لىل فلد تانايب لاسرال رايختالال.
- **Password:** ددح **Password** ةناخ ددح. لىل فلد نزم لىل لىل فلد تانايب لاسرال رايختالال.
- **Confirm:** ددح **Confirm** ةناخ ددح. لىل فلد نزم لىل لىل فلد تانايب لاسرال رايختالال.

(يرايختالال) شالفلال مجح

يلخدالال تاقوملا نزم لىل لىل فلد تانايب لاسرال رايختالال. لىل فلد نزم لىل لىل فلد تانايب لاسرال رايختالال.

- **Flash:** ددح **Flash** ةناخ ددح. لىل فلد نزم لىل لىل فلد تانايب لاسرال رايختالال.
- **Maximum Flash to be used by Logging(KB):** ددح **Maximum Flash to be used by Logging(KB)** ةناخ ددح. لىل فلد نزم لىل لىل فلد تانايب لاسرال رايختالال.
- **Minimum free Space to be preserved(KB):** ددح **Minimum free Space to be preserved(KB)** ةناخ ددح. لىل فلد نزم لىل لىل فلد تانايب لاسرال رايختالال.

<ul style="list-style-type: none"> ARP Inspection Banner External Authentication Fragment Settings HTTP ICMP Secure Shell SMTP Server SNMP Syslog Timeouts Time Synchronization 	<p>Logging Setup Logging Destinations Email Setup Event Lists Rate Limit Syslog Settings Syslog Servers</p> <p>Basic Logging Settings</p> <p>Enable Logging <input checked="" type="checkbox"/></p> <p>Enable Logging on the failover standby unit <input checked="" type="checkbox"/></p> <p>Send syslogs in EMBLEM format <input checked="" type="checkbox"/></p> <p>Send debug messages as syslogs <input checked="" type="checkbox"/></p> <p>Memory Size of the Internal Buffer <input type="text" value="4096"/> (4096-52428800 Bytes)</p> <p>Specify FTP Server Information</p> <p>FTP Server Buffer Wrap <input checked="" type="checkbox"/></p> <p>IP Address* <input type="text" value="WINS1"/></p> <p>Username* <input type="text" value="admin"/></p> <p>Path* <input type="text" value="/var/ftp"/></p> <p>Password* <input type="password" value="....."/></p> <p>Confirm* <input type="password" value="....."/></p> <p>Specify Flash Size</p> <p>Flash <input type="checkbox"/></p> <p>Maximum Flash to be used by Logging(KB) <input type="text" value="3076"/> (4-8044176)</p> <p>Minimum free Space to be preserved(KB) <input type="text" value="1024"/> (0-8044176)</p>
--	--

عدبل **Deploy** رقناو، تاريخيغتل قيبطت ديرت شيح FTD زاهج رتخاو، رايخل **Deploy** رتخأ. يساسأل ماظنل دادعإ ظفحل **Save** رقنا يساسأل ماظنل دادعإ رشن.

ثادحلأل مئاوق

لماع ي ف اهنيمضت متيس يتل لجلسل تانايب ديحتو ثادحلأل ةمئاق ريرحت/ءاشناب ثادحلأل مئاوق نيوكت رايخ كل حمسي لجلسل تاهجو نمض لجلسل ةيفصت لماع نيوكت دنع ثادحلأل مئاوق مادختسا نكمي. ثادحلأل ةمئاق ةيفصت

ةصصخملم ثادحلأل مئاوق فئاظو مادختسال نيرايخ ماظنل حيي.

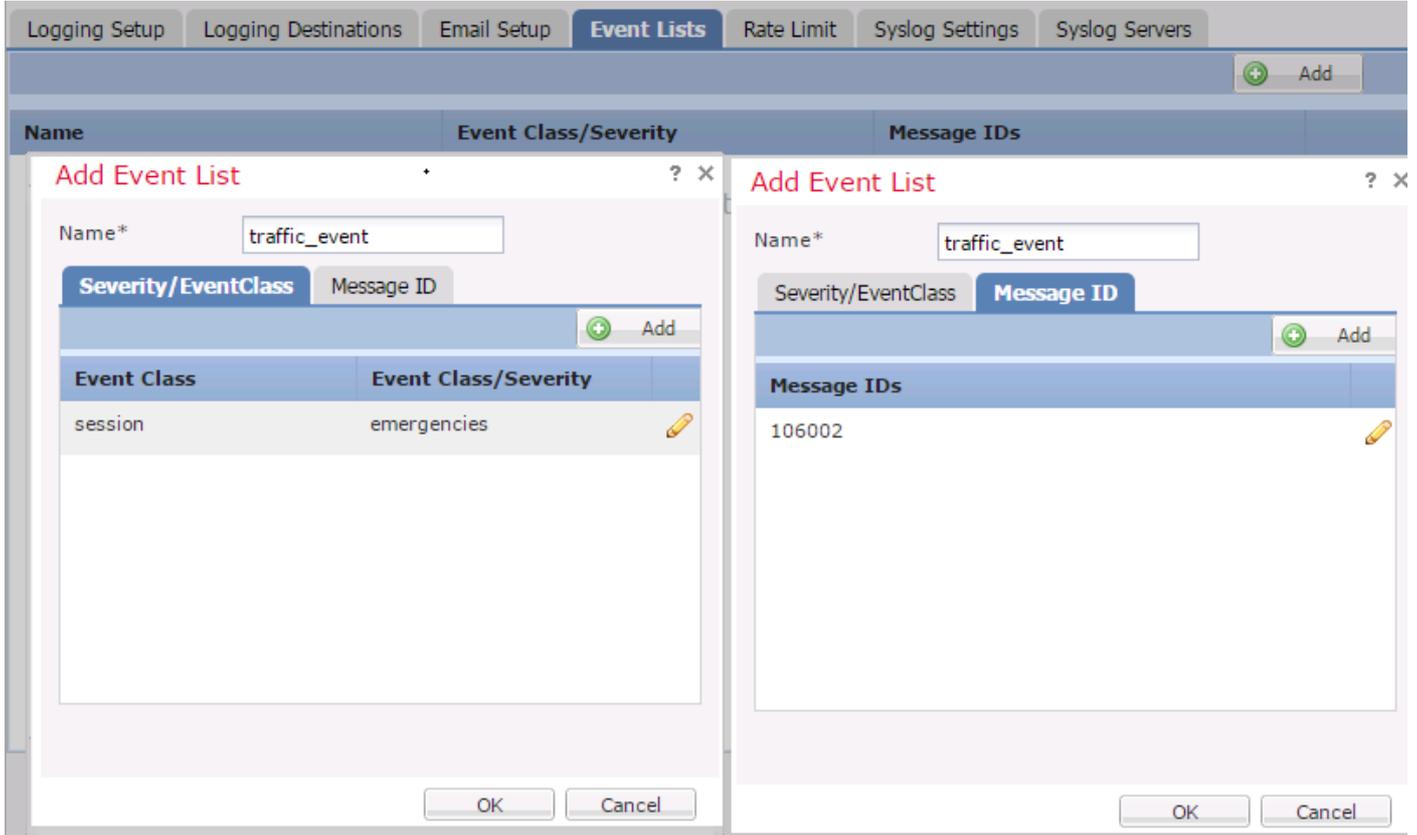
- ةروطخلأل ةئفلا
- ةلاسرل فرعم

هذه **Add** قوف رقناو **Event List > Syslog > Threat Defense Policy > Platform Setting > Device** رتخأ، ةصصخم ثادحلأل مئاوق نيوكتل تارايلأل يه:

- Name: ثادحلأل ةمئاق مسا لخدأ.
- Severity/Event Class: **Add** قوف رقنا، ثدحلأل/ةروطخلأل ةئف مسا ق ي ف.
- Event Class: ةومجم "ثدحلأل ةئف" فرعت. اهديرت يتل لجلسل تانايب عونل ةلدسنملا ةمئاقلا نم ثدحلأل ةئف رتخأ. تازيمل سفن لثمت يتل **syslog** دعاقو نم.

لمعلال ةسلجبل قلعنتت يتل **syslogs** عيجم نمضتت يتل لولمعلال ةسلجلل ثدحلأل ةئف كانه، لالملا ليلبس يلعل.

- Syslog Severity: عرّف مستوى شدة الرسائل التي سيتم تسجيلها. (الخطوة 7 من إعدادات الحدث).
- Message ID: رقم إضافي للرسالة، يُستخدم لتمييز الرسائل المتعددة لنفس الحدث. (الخطوة 7 من إعدادات الحدث).
- Message IDs: قائمة من معرفات الرسائل التي سيتم تسجيلها.



لليكشنتال تذقنأ **OK** تقطقط.

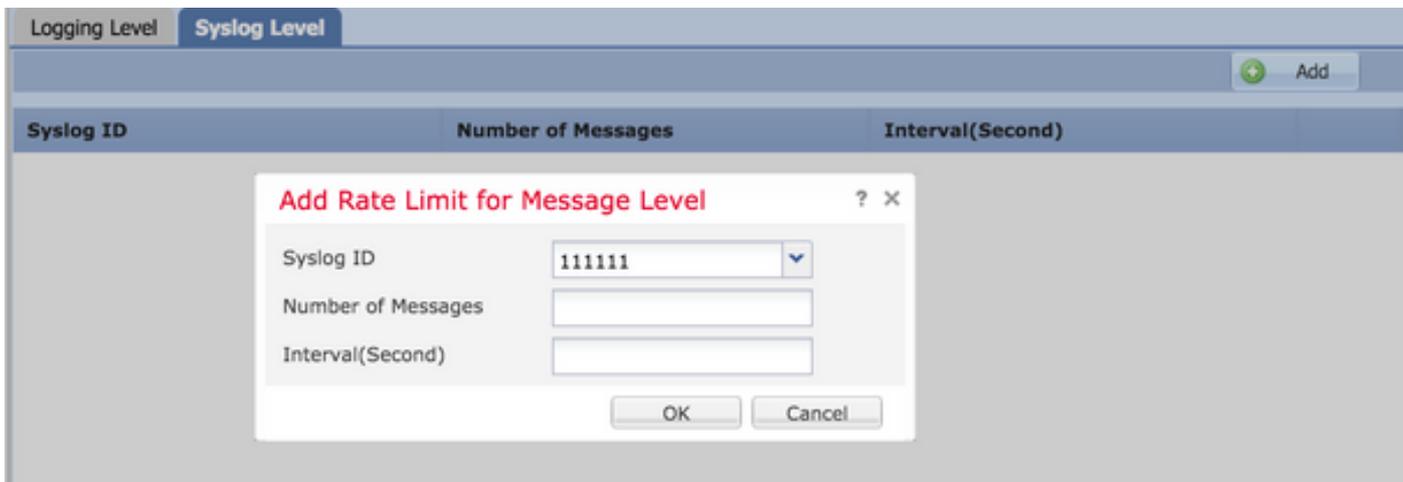
عدبل **Deploy** رقناو، تاريخيغثال قيبطت ديرت شيح FTD زاه رتخأ **Deploy**، ديرت ام رتخأ. يساسألماظنلدادعإطفحل **Save** رقنا يساسألماظنلدادعإرشن.

لدعملالديدحت Syslog

ديرت يتالالاسرلالعروطخدديواهنويوكتم يتالتاهجولاعيمجىلالالاسرلانىيتاللائسرلالدعملالده رايخ ددي اهللدعملالدودحنبيغث.

نارايخ كيديل. **Device > Platform Setting > Threat Defense Policy > Syslog > Rate Limit** رتخأ، عصصخم شادجأ مئوق نبيوكتل:لدعملالده نبيغثكننكمي امهيلىل دننتست:

- ليحسثالايوتسم
- Syslog تايوتسم



ليكشت يوتسم syslog ال تذقنأ in order to OK تقطقط

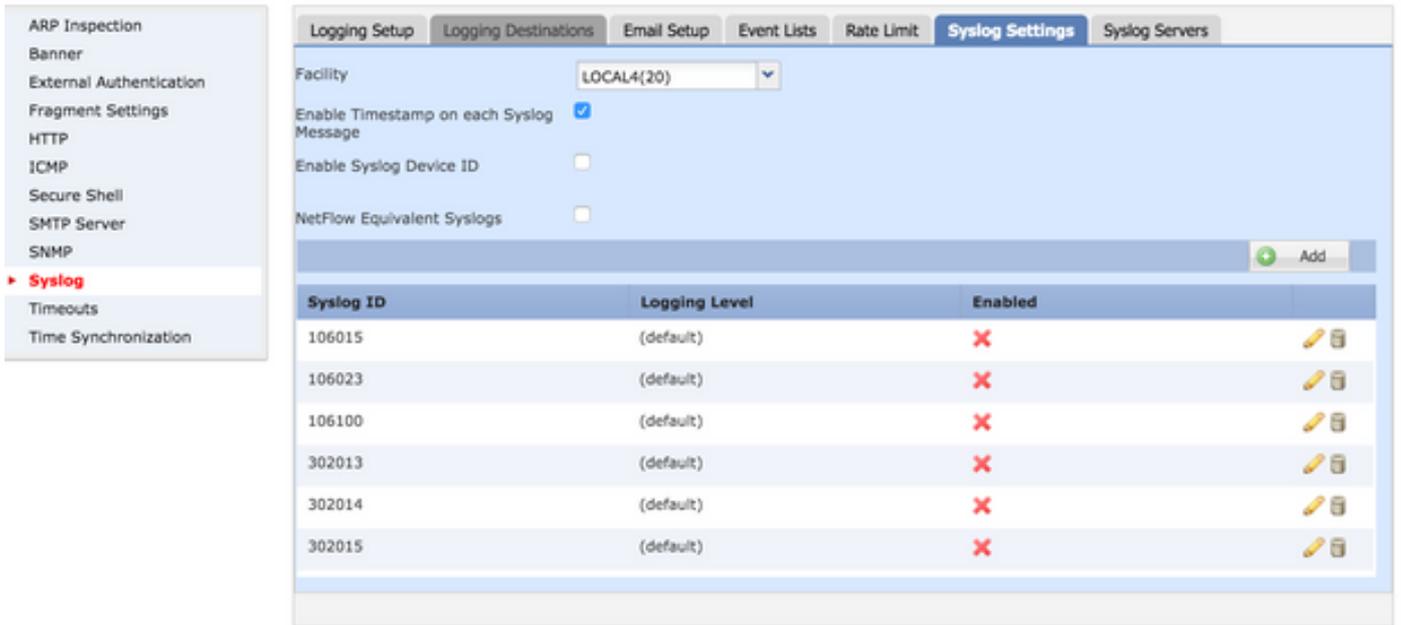
عدبل Deploy رقناو، تاريغيغتلا قيبطت ديرت شيح FTD زاه رتخأ Deploy، ديرت ام رتخأ. يساسألماظنلا دادع| ظفح Save رقنا يساسألماظنلا دادع| رشن

Syslog تادادع|

لئاسري في ينمزللا عباطلا نيمضت اضيأ كنكمي. Syslog لئاسري في Facility ميق نيوكت نيمضت Syslog تادادع| حيتت syslog. مداخل ةصاخلا رخألا تاملعمل او لجلسلا

Device > Platform Setting > Threat Defense Policy > Syslog > Syslog Settings. رتخأ، ةصصخم ثادحأ مئاوق نيوكتل

- Facility: لئاسرلا عم لماعتلا نكمي. ةلاسرلا ليحستب موقوي يذلا جم انربلا عون ديدحتل قفرم دوامادختسا متي: Facility. ةأشنملا ةميقرتخأ، ةلدسنملا Facility ةمئاقلا نم. فلتخم لكشب ةفلتخمل قفارملا تاذ
- Enable Timestamp on each Syslog Message: نيمضتل رايخالا Enable Timestamp on each Syslog Message ةناخ دح Syslog لئاسري في ينمزللا عباطلا
- Enable Syslog Device ID: ريغ syslog لئاسري في زاهجلا فرعم نيمضتل رايخالا Enable Syslog Device ID ةناخ دح. راعش قيسنتب
- Netflow Equivalent Syslogs: نأ نكمي. NetFlow ل ةئفكمل Syslog لئاسرلا رايخالا Netflow Equivalent Syslogs ةناخ دح. زاهجال عادأ يلع رثؤي
- رايخالا Syslog ID/ Logging Level عبرم ددحو Add رقنا، فياضالا syslog فرعم ديدحتل: ددحم syslog فرعم ةفاضلا



عدبل **Deploy** رقناو، تاريغيغتلا قيبيطت ديتر شيح FTD زاهج رتخ **Deploy**، ديتر ام رتخأ. يساسألماظنلاداع| ظفحل **Save** رقنا يساسألماظنلاداع| رشن

يحلحمل ليجستلا نيوكت

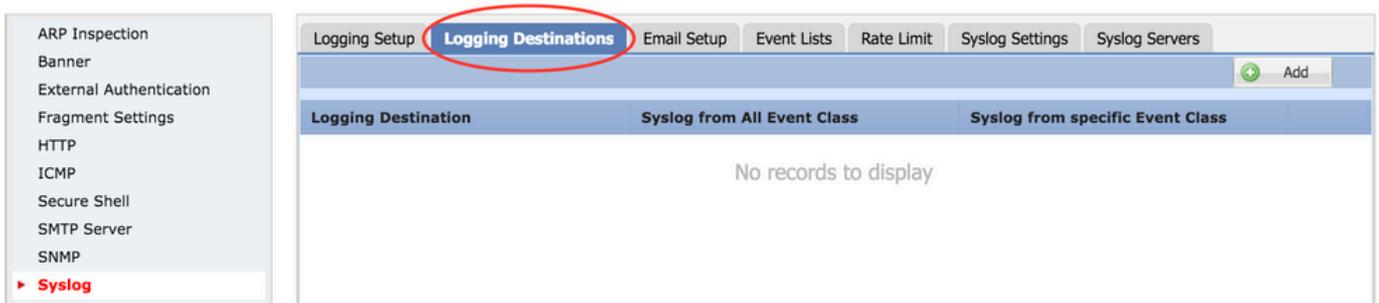
ةدحمتاهجو ىل ليجستلا نيوكتل ليجستلا هجو مسق مادختسا نكمي

ي: هةرفومتلا ةيلخادلا ليجستلا تاهجو

- (ليجستلا اتقؤم نزملا) ييلخادلا ليجستلا اتقؤملا نزملا يي ةدوجوملا تالجسلا: ييلخادلا اتقؤملا نزملا
- (ليجستلا مكحت ةدحو) مكحتلا ةدحو ىل تالجسلا لسري: مكحتلا ةدحو
- (ةيفرطالا ةبقارملا) SSH تاسلج ىل Syslog ليجست: SSH تاسلج

يحلحمل ليجستلا نيوكتل تاوطخ ثالث كانه

الخطا 1. **Device > Platform Setting > Threat Defense Policy > Syslog > Logging Destinations**



الخطا 2. **logging destination** دحمل ليجست ةيفصت لماع ةفاضال **Add** رقنا. ةوطخلا

وأمكنك تحديث أو إيقاف تشغيل أو تغيير إعدادات تسجيل الأحداث في **Logging Destination** قائمة من إعدادات النظام. يمكنك تغيير إعدادات تسجيل الأحداث في SSH.

من إعدادات النظام، يمكنك تغيير إعدادات **Event Class** قائمة من إعدادات النظام. يمكنك تغيير إعدادات **Event Class** قائمة من إعدادات النظام. يمكنك تغيير إعدادات **Event Class** قائمة من إعدادات النظام.

- Filter on Severity: يمكنك تغيير إعدادات **Filter on Severity** قائمة من إعدادات النظام.
- User Event List: يمكنك تغيير إعدادات **User Event List** قائمة من إعدادات النظام.
- Disable Logging: يمكنك تغيير إعدادات **Disable Logging** قائمة من إعدادات النظام.

7 إلى (إعدادات النظام) 0 من إعدادات النظام. يمكنك تغيير إعدادات **Event Class** قائمة من إعدادات النظام. يمكنك تغيير إعدادات **Event Class** قائمة من إعدادات النظام.

Add Logging Filter

Logging Destination: Internal Buffer

Event Class: Filter on Severity (Secondary: emergencies)

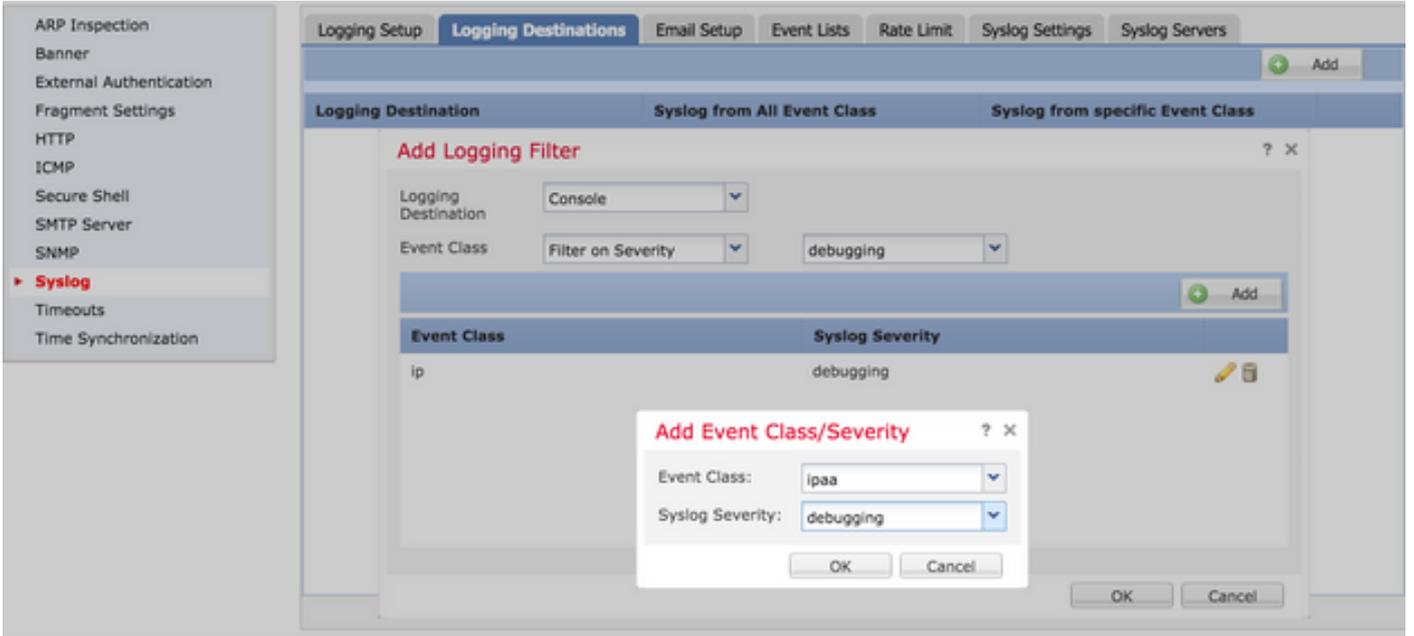
Event Class	Syslog Severity
No records to display	

Buttons: Add, OK, Cancel

Add قوف رقنا، اذة ليجستال ايفصت لماع إلى اةلصف نم شح ةئف ةفاضل 3. ةوطخل

Event Class: ةلءس نم "شءل ةئف" رءء: Event Class

ةلءس نم **Syslog Severity** ةمءلءل نم Syslog ةروطء رءء: Syslog Severity



ةددحم ليجست ةهجول ةيفصتلا لماع ةفاضال ةيفصتلا لماع نيوكت درجم OK رقنا

رشن عدبل Deploy رقناو، تاريغتلا قيبطت ديرت شيح FTD زاغ رتخأ، Deploy رتخأ. ياساسألماظنلا دادع| ظفح Save رقنا ياساسألماظنلا دادع

يجراخل ليجستلا نيوكت

جيراخل ليجستلا نيوكتل Device > Platform Setting > Threat Defense Policy > Syslog > Logging Destinations.

هذه يجراخل ليجستلا عاونأ FTD معددي

- دع ب نع Syslog مداخ ىلا تالجسلا لسري Syslog مداخ.
- ةمئالم كجراخل لالجسلا لسري: SNMP ةمئالم.
- اقبس مهن نيوكت مت ديرت ليجستل مداخ مداختساب ينورتكلالال ديربال ربع تالجسلا لسري: ينورتكلالال ديربال.

م تي يذلا ليجستلا عون ليجستلا تاهج وديجت دح. هسفن وه يلخادلا ليجستلاو يجراخل ليجستلاب صاخلا نيوكتلا ديعبال مداخل ىلا "ةصصخملا ثادحلأا" مئوق ىلا ادانتسا "ثادحلأا تائف" نيوكت نكمملا نم. هذيفنت

دع ب نع Syslog مداخ

FTD لوكوتورب نم دع ب نع اهنينختو تالجسلا ليجستلا Syslog مداوخ نيوكت نكممي

ةديعبال syslog مداوخ نيوكتل تاوطخ ثالث كانه

1. ةوطخل Device > Platform Setting > Threat Defense Policy > Syslog > Syslog Servers رتخا.

2. ةوطخل syslog مداخ بةلصل تا ذمةلمال نيوكتب مق.

• يف TCP syslog مداخل رشن مت اذا: ال طعم TCP syslog مداخل نوكي ام دنع رورم لاب مدختس ملام رورم ةكرحل حامسلا
 نوكي ام دنع طقف قبطني اذهو. ASA ربع ةكباشلا رورم ةكرح ضفر متيسف ، لوصولل لباق ريغ وهو ةكباشلا
Allow user traffic to pass when TCP syslog server is down ةناخ دح TCP. وه syslog مداخلو ASA نيب لقنلا لوكوتورب
 ال طعم syslog مداخل نوكي ام دنع ةهجاو لالخال نم رورم لاب رورم ل ةكرحل حامسلا ل رايخال

• مداخل نوكي ام دنع FTD يف فطصت يتلا لئاسرلا دنع وه لئاسرلا راطتنا ةمئاق مچح: لئاسرلا راطتنا ةمئاق مچح
 0 ناك اذا. ةدحاو ةلاسرو وه ىندال دحاو ةلاسرو 512 وه يضارفال. لئاسر ي لبق ي الو الو الوغشم ديعبلا syslog
 .دوحم ريغ ربتعي راطتنا ل ةمئاق مچح ناف ، رايخال اذه يف ادحم

3. ةوطخال Add قوف رقنا ، ةديعبلا syslog مداخل ةفاضال .

IP Address: مداخل Syslog مداخل يوتحي ةكباش نئاك رتخأ ، ةلدسنم ل IP Address ةمئاقلا نم
 .ديج نئاك عاشنال (+) دئاز ةنوقي رقنا ، ةكباش نئاك

Protocol: Syslog لاصتال رايخال رز UDP وأ TCP رز ىلع ام رقنا

Port: 514 وه ، ايضارفتا . Syslog مداخل ذفنم مقرر لخدأ

Log Messages in Cisco EMBLEM format (UDP only): رايخال ةناخ Log Messages in Cisco EMBLEM format (UDP only) قوف رقنا :
 UDP ىلى ةدنتس ملام syslog ىلى قبطني اذه Cisco راعش قيسننتب لئاسرلا ليجستل ابولطم ناك اذا رايخال اذه نيكم تل
 طقف

Available Zones: "ةدح ملام تاهجاو ل / قطانم ل" دومع ىلى هلقناو syslog مداخل ىلى اهلخال نم لوصولو نكمي يتلا نامألا قطانم لخدأ

Add Syslog Server



IP Address*

Protocol TCP UDP

Port (514 or 1025-65535)

Log Messages in Cisco EMBLEM format(UDP only)

Available Zones

Selected Zones/Interfaces

ليكش التل تذقن أن **OK** و **Save** in order to تقطط.

رشن عدبل **Deploy** رقن او، تاريخي غتال قيبطت ديرت شيح FTD زاهج رتخأ، **Deploy** رتخأ. سيسأل ال ماظنل دادع| ظفحل **Save** رقن ا سيسأل ال ماظنل دادع|

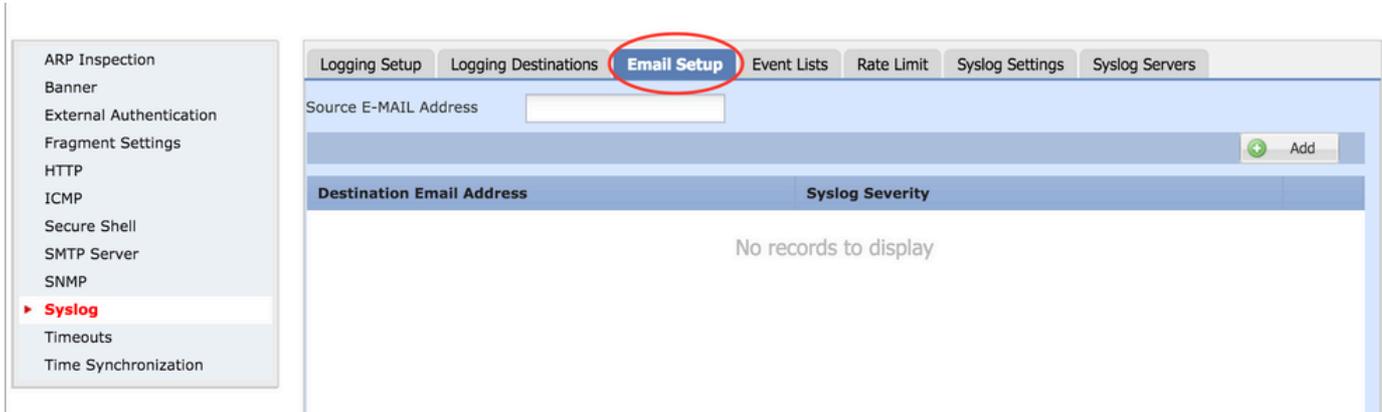
ليجست لل ينورتكل الال ديربل دادع|

يف طقف ليجست هجوك ينورتكل الال ديربل مادختس| نكمي. ددحم ينورتكلال ديرب ناونع ال syslog لاسراب كل FTD حمسي لعلفالاب ينورتكلالال ديربل ليجرت مداخل نيوكت ةلاح.

syslogs. ل دادع| ةيلمع ينورتكلال ديرب لكشي نأ steps نانثا كانه.

رتخا. 1. ةوطخلال **Device > Platform Setting > Threat Defense Policy > Syslog > Email Setup**

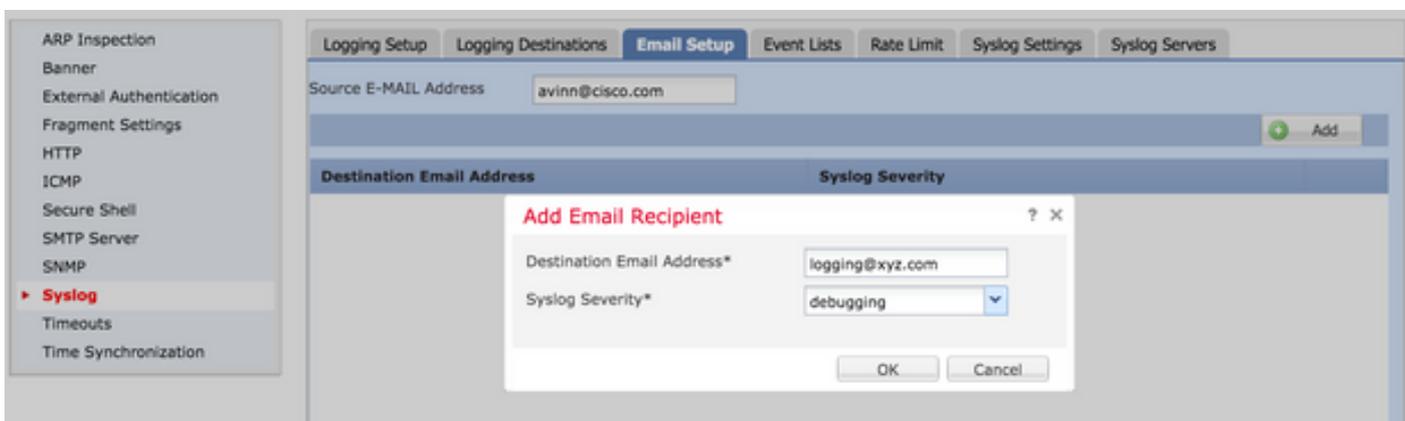
نم ةل سرملال ينورتكلالال ديربل لئاسر ةفاك ال ع رهظي ذل رصم ال ينورتكلالال ديربل ناونع لخدأ: Source E-MAIL Address: syslogs. ال ع يوتحت يتال او FTD



2. عروطخ syslog و ناو نع ينورتكلال ديرب ةيغال تللكش in order to عروطخ 2.

Destination Email Address: syslog لئاسر لاسرلا م تي شيح ةهجولا ينورتكلال ديربلا ناو نع لخدأ

Syslog Severity: ةلدسنملا Syslog Severity ةمئاقلا نم Syslog ةروطخ رتخأ



ليكشتلا تذقنأ in order to OK ترقط

رشن عدبل Deploy رقناو، تاريغيغتلا قيبطت ديرت شيح FTD زاغ رتخأ، Deploy رتخأ. يساسأل اماظنلا دادعإ ظفح Save رقنا يساسأل اماظنلا دادعإ

ةحصلا نم ققحتلا

نيوكتلا اذه ةحص نم ققحتلل ءارجإ آيلاج دجوي ال

اهالصال ءاطخأل فاشكتسا

اهالصال نيوكتلا ءاطخأل فاشكتسال اهمادختسا كنك م ي تامولعم مسقلا اذه رفوي

- system لخدأو، FTD ةرادإ ةهجاو ىلل لوخدلا ليحس تب مق FTD نم رماوأل رطس ةهجاو يف FTD syslog نيوكت نم ققحت ةيضيخشثلا رماوأل رطس ةهجاو يف مكحتلا ةدحول رمالا **support diagnostic-cli**

```
> system support diagnostic-cli
Attaching to ASA console ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
```

```
><Press Enter>
firepower# sh run logging
logging enable
logging console emergencies
logging buffered debugging
logging host inside 192.168.0.192
logging flash-minimum-free 1024
logging flash-maximum-allocation 3076
logging permit-hostdown
```

- نم ققحت و SSH ربع FTD ةرادا ةهجاو ىل ل وخذل ليجستب مق FTD نم syslog مداخل ل لوصول ةيناكم نم دكأت رمأل ping مادختساب لاصلتال

```
Copyright 2004-2016, Cisco and/or its affiliates. All rights reserved.
Cisco is a registered trademark of Cisco Systems, Inc.
All other trademarks are property of their respective owners.
Cisco Fire Linux OS v6.0.1 (build 37)
Cisco Firepower Threat Defense for VMWare v6.0.1 (build 1213)
```

```
> system support diagnostic-cli
Attaching to ASA console ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
firepower> en
Password:
firepower# ping 192.168.0.192
```

- ىل ل وخذل ليجستب مق ل.دان syslog ل او FTD ل نيب ةي لوصول مالتقق د in order to ىلع طبر تذخأ عيطتسي تنأ [طاقتل](#) ىل عجرا، ةمزحل طاقتل رمأو ىل لوصول ل **system support diagnostic-cli** رمأل لخدأو SSH ربع FTD ةرادا ةهجاو [ASDM](#) نيوكت للاثم و [CLI](#) مادختساب [ASA](#) ةمزح
- حاجنب جهنل رشن قيبطت نم دكأت

ةلص تاذا تامولعم

- [ASA ل Cisco نم FirePOWER ديدهت نعا فدلل عيرسلا عدبلا ليلد](#)
- [Cisco Systems - تادنتس مل او ينقتال معدل](#)

ةمچرتل هذه لوج

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