

FMC ربع FTD ىلع ليجستلا نيوكت

تايوت حمل

[قم دق م ل](#)

[ةيساس أال تابل طت م ل](#)

[تابل طت م ل](#)

[ةمدخت س م ل تانوك م ل](#)

[ةيساس أ تامول عم](#)

[نيوكت ل](#)

[ماع ل syslog نيوكت نيوكت](#)

[ليجستلا دادع](#)

[ثادخال مي اوق](#)

[لدع م ل ديخت Syslog](#)

[تادادع Syslog](#)

[يلج م ل ليجستلا نيوكت](#)

[يجراخل ليجستلا نيوكت](#)

[دعب نع Syslog مداخ](#)

[ليجستلا نيوكت نيوكت ل ديابل دادع](#)

[قحص ل نم ققحت ل](#)

[اهخالص او عاخالص فاشكت س](#)

[قحص تاذ تامول عم](#)

ةمدق م ل

J- FirePOWER Threat Defense (FTD) J- Firepower Management Center (FMC) لوخدل ليجست نيوكت دنت س م ل اذه فص ي

ةيساس أال تابل طت م ل

تابل طت م ل

ةيلال عيضاوم ل ابة فرعم كيديل نوكت نأب Cisco ي صوت:

- FirePOWER ةينقت
- (ASA) ةلدع م ل نام أال ةزهجأ
- Syslog لوكوتورب

ةمدخت س م ل تانوك م ل

ةيلال ةيدام ل تانوك م ل او جم اربال تارادص ل دنت س م ل اذه ي ةدراول تامول عم ل دنت س ت

- ASA Firepower ل ASA (5506X/5506H-X/5506W-X، ASA 5508-X، ASA 5516-X) ل تال ل م عت ي تال ل (6.0.1 جم ان ربال رادص ل م عت ي تال ل)

- شذألأ تارادصلإل او جم انربلأ 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. (يضارتفا) حوسمم نيوكتب دنتسملأ اذف يف ةمدختسملأ ةزهجالأ عيمج تادب رمأ يأل لمحتحملأ ريثأتلل كمهف نم دكأتف ،لغشتلأ ديق كتكبش

ةيساسأ تامولعم

هئاطخأ فاشكتساو FTD زاهج ةبقارمل ةمزالل تامولعملأ FTD ماظن تالجس كل رفوت اهالحصاو.


ثداوخلأ ةجلعم يفو ينيورتور لكشب اهالحصاو ءاطخأ فاشكتسا يف ةديفم تالجسلأ دعت ءاوس دح ىلع يجرأخلل او يلحملأ ليجستلأ FTD زاهج معدف. ءاوس دح ىلع

يجرأخلل ليجستلأ. اهالحصاو live ءاطخأ فاشكتسا ىلع يلحملأ ليجستلأ كدعاسي نأ نكمي يجرأخلل syslog مداخل ل FTD زاهج نم تالجسلأ عمجل ةقيرط وه

دعاسي نأ نكمي. تاهي بنتلأو تالجسلأ عيمجت يف يزكرم مداخل ل ليجستلأ دعاسي ثداوخلأ ةجلعمو لجال طابترا يف يجرأخلل ليجستلأ

يلخادلأ تقؤملا نزملاو مكحتلأ ةدحو رايف FTD زاهج معدف ،يلحملأ ليجستلأ ةبسنلاب Secure Shell (SSH) لعم ةسلج ليجستو

ديربلل ليحرت مداخلو يجرأخلل syslog مداخل FTD زاهج معدف ،يجرأخلل ليجستلأ ةبسنلاب ينيورتكللإل

 ديدحت/ليجستلأ عون ىلإ هبتنا ،زاهجال ربع ةريبك رورم ةكرح ترم اذأ: ءظحالما رادج ىلع ريثأتلأ بنجتف يذلأو ،تالجسلأ ددع ديدحتل ءارجلأ اذف مق .لدملأ/ةروطخلأ ةيامحل

نيوكتلأ

ةمالع Platform Settings ىلإ لاقتنالأ دنع ليجستلأ ةقلعتملأ تانيوكتلأ عيمج نيوكت نكمي ةروصلأ هذف يف حضوم وه امك Devices > Platform Settings رتخأ. بيبوتلأ ةمالع Devices لفسأ بيبوتلأ

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 ةنوقفأ 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

ةروصول 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

Add to Policy

Save Cancel

ماعال syslog نيون نيونكت

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

ليجستلا دادع

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

رتخأ . Syslog > Logging Setup

يساسأل ليجستلا دادع

- **Enable Logging:** ددح **Enable Logging** ةناخ ددح. ليجسستلا نيكمتل رايختالا
- **Enable Logging on the failover standby unit:** ددح **Enable Logging on the failover standby unit** ةناخ ددح. نيوكتل رايختالا لوجدل ليجست رفاوتلا ةناخ ددح.
- **Send syslog in EMBLEM format:** ددح **Send syslog in EMBLEM format** ةناخ ددح. راعشك syslog قيسنت نيكمتل رايختالا ةناخ ددح. اذه قفاوتي. CiscoWorks (RME) دراوم ةرادال Syslog لرحمل سيسئركش راعشلا قيسنت مادختسا متي. ةهجو ل لك لطق رفاوتي. تالوحو لواتاهووملا ةطساوب هجاتن مت يذلا Cisco IOS Software جمانربل Syslog قيسنت عم قيسنتلا ل UDP syslog مداوخل
- **Send debug messages as syslogs:** ددح **Send debug messages as syslogs** ةناخ ددح. عاطخال احيصت تالجس لاسرال رايختالا **Send debug messages as syslogs** ةناخ ددح. Syslog مداخ ل لئاسرك
- **Memory size of the Internal Buffer:** ددح **Memory size of the Internal Buffer** ةناخ ددح. لرحسلا تانايب ظفح FTD ل نكمي شيخ لخدال تقووملا ةركاذلا نزم مجح لخدأ. تقووملا نزملا دح ل لوصولا مت اذ لرحسلا تانايب ريودت متي.

(يرايختا) FTP مداخ تامولعم

يلخدال تقووملا نزملا لادبتسا موقت نأ لبق FTP مداخ ل لرحسلا تانايب لاسرا ديرت تنك اذ FTP مداخ ل لوصافت ددح

- **FTP Server Buffer Wrap:** ددح **FTP Server Buffer Wrap** ةناخ ددح. FTP مداخ ل لخدال تقووملا نزملا لرحسلا تانايب لاسرال رايختالا
- **IP Address:** ددح **IP Address** ةناخ ددح. FTP مداخ ل لخدال تقووملا نزملا لرحسلا تانايب لاسرال رايختالا
- **Username:** ددح **Username** ةناخ ددح. FTP مداخ ل لخدال تقووملا نزملا لرحسلا تانايب لاسرال رايختالا
- **Path:** ددح **Path** ةناخ ددح. FTP مداخ ل لخدال تقووملا نزملا لرحسلا تانايب لاسرال رايختالا
- **Password:** ددح **Password** ةناخ ددح. FTP مداخ ل لخدال تقووملا نزملا لرحسلا تانايب لاسرال رايختالا
- **Confirm:** ددح **Confirm** ةناخ ددح. FTP مداخ ل لخدال تقووملا نزملا لرحسلا تانايب لاسرال رايختالا

(يرايختا) شالفلدا مجح

يلخدال تقووملا نزملا لادبتسا موقت نأ لبق FTP مداخ ل لرحسلا تانايب لاسرا ديرت تنك اذ FTP مداخ ل لوصافت ددح

- **Flash:** ددح **Flash** ةناخ ددح. لخدال تقووملا نزملا لرحسلا تانايب لاسرال رايختالا
- **Maximum Flash to be used by Logging(KB):** ددح **Maximum Flash to be used by Logging(KB)** ةناخ ددح. لخدال تقووملا نزملا لرحسلا تانايب لاسرال رايختالا
- **Minimum free Space to be preserved(KB):** ددح **Minimum free Space to be preserved(KB)** ةناخ ددح. لخدال تقووملا نزملا لرحسلا تانايب لاسرال رايختالا

<ul style="list-style-type: none"> ARP Inspection Banner External Authentication Fragment Settings HTTP ICMP Secure Shell SMTP Server SNMP <li style="background-color: #e0e0e0;">▶ Syslog Timeouts Time Synchronization 	<div style="border: 1px solid #ccc; padding: 5px;"> <div style="display: flex; border-bottom: 1px solid #ccc;"> <div style="background-color: #4a7ebb; color: white; padding: 2px 5px; font-weight: bold;">Logging Setup</div> <div style="padding: 2px 5px; font-weight: bold;">Logging Destinations</div> <div style="padding: 2px 5px; font-weight: bold;">Email Setup</div> <div style="padding: 2px 5px; font-weight: bold;">Event Lists</div> <div style="padding: 2px 5px; font-weight: bold;">Rate Limit</div> <div style="padding: 2px 5px; font-weight: bold;">Syslog Settings</div> <div style="padding: 2px 5px; font-weight: bold;">Syslog Servers</div> </div> <div style="padding: 10px;"> <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> </div> </div>
--	---

عدبل **Deploy** رقناو، تاريخيغلتا قيبطت ديرت شيح FTD زاهج رتخاو، رايخل **Deploy** رتخأ. يساسألماظنلا دادعإ ظفحل **Save** رقنا يساسألماظنلا دادعإ رشن.

ثادحلألماوق

لماع يفي اهنيمضت متيس يتلا لجلسل تانايب ديحتو ثادحلألماوق ريرحت/عاشنا ب ثادحلألماوق نيوكت رايخ كل حمسي لجلسلتا تاهجو نمض لجلسلتا لصفصت لماع نيوكت دنع ثادحلألماوق مادختسا نكمي. ثادحلألماوق لصفصت

ةصصخلمل ثادحلألماوق فئاظو مادختسال ني رايخ ماظنلا حيتي

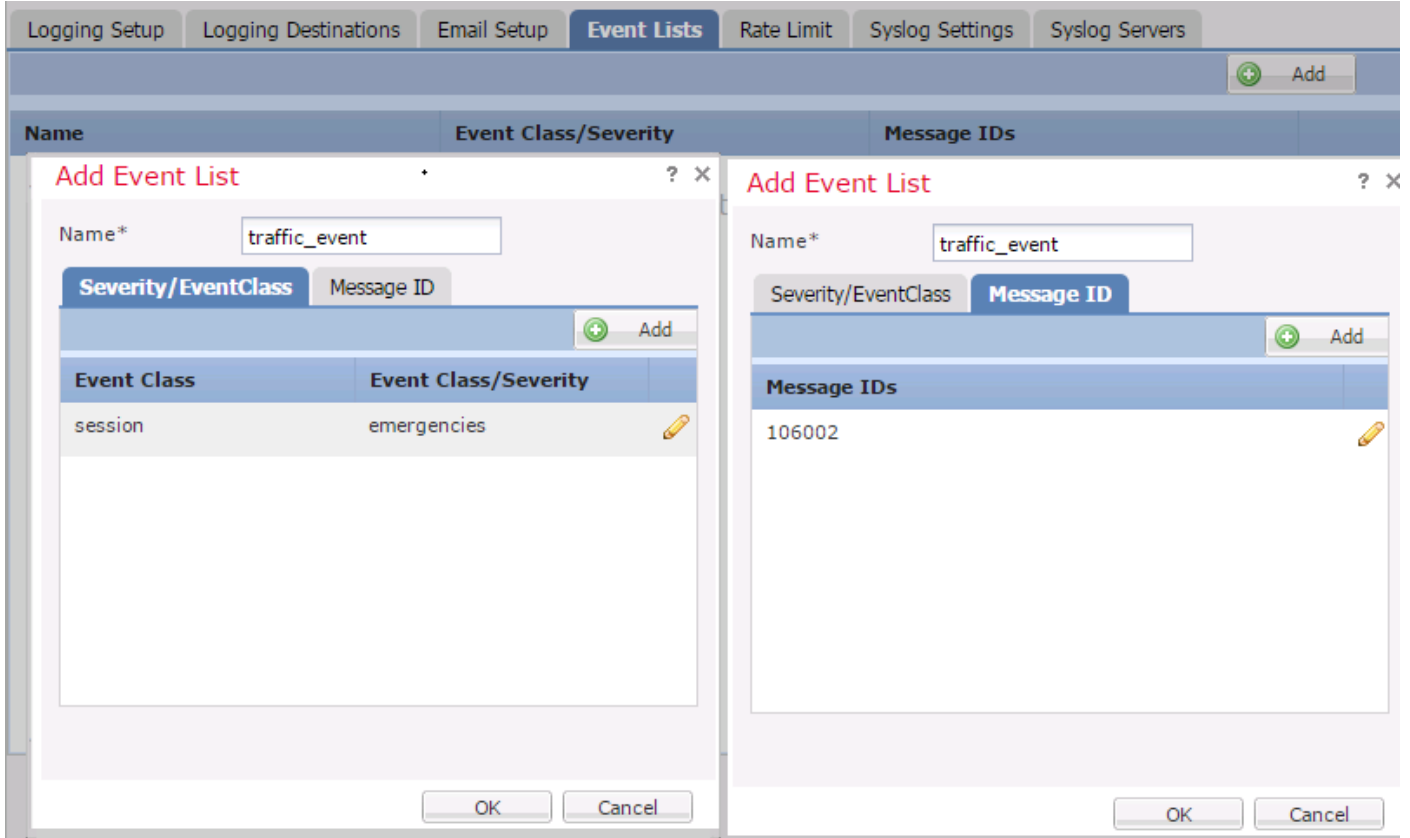
- ةروطخلألماوق
- ةلاسرل فرعم

هذه **Add** قوف رقناو **Event List > Syslog > Threat Defense Policy > Platform Setting > Device** رتخأ، ةصصخلمل ثادحلألماوق نيوكتل تارايلال يه:

- Name: ثادحلألماوق مسال خدأ
- Severity/Event Class: **Add** قوف رقنا، ثدحلألماوق لصفصت مسق يفي
- Event Class: ةومجم "ثدحلألماوق" فرعت. اهديرت يتلا لجلسل تانايب عونل ةلدسنملا ةمئاقلا نم ثدحلألماوق رتخأ: Event Class. تازيمل سفن لثمت يتلا syslog دعاقو نم

لمعلال ةسلج قلعنت يتلا syslogs عيمج نمضت يتلاو لمعلال ةسلجل ثدحلألماوق كانه، لالمال ليلبس يلع

- Syslog Severity: عرّف مستوى شدة الرسائل التي سيتم تسجيلها. (الخطوة 7 من إعدادات Syslog Severity).
- Message ID: رقم إضافي يميز الرسائل التي سيتم تسجيلها. (الخطوة 7 من إعدادات Message ID).
- Message IDs: قائمة من الأرقام التي سيتم تسجيلها.



لإكمال العملية، انقر على **OK** في أسفل النافذة.

بعد ذلك، انقر على **Deploy** في أعلى اليمين، ثم انقر على **Save** في أعلى اليمين. سيؤدي ذلك إلى تطبيق الإعدادات.

إعدادات Syslog

يتم إعداد إعدادات Syslog في صفحة **Device > Platform Setting > Threat Defense Policy > Syslog > Rate Limit**. انقر على **Rate Limit** في أعلى اليمين.

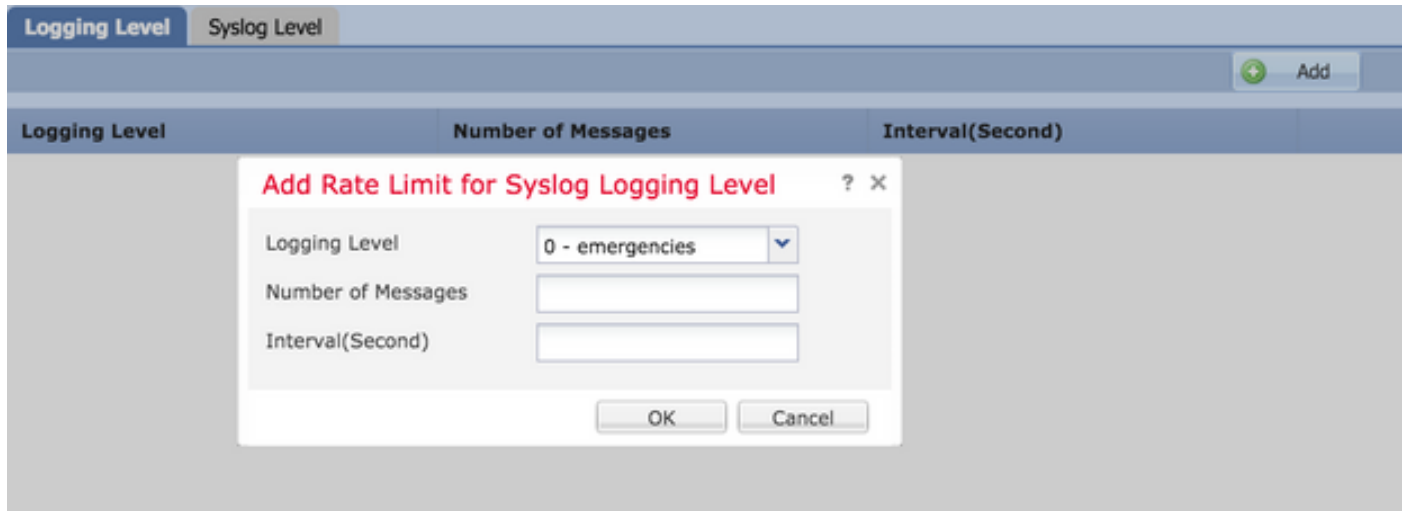
لإعداد إعدادات Syslog، انقر على **Device > Platform Setting > Threat Defense Policy > Syslog > Rate Limit**. انقر على **Rate Limit** في أعلى اليمين.

- إعدادات Syslog
- إعدادات Syslog

Add. قوف رقناو Logging Level رتخأ، ليجستال يوتسم ىل اذنتسم ل دعمال دح نيكم تل

- Logging Level: هه ل دعمال دي دحت اءرچ اذرت يذال ليجستال يوتسم رتخأ، ءلدسنم Logging Level ءم اقلال نم
 - Number of Messages: ءد دعمال ءنمزلال ءرتفلال لال خ اءقلا متيس يتال syslog لئاسر دءل صقأال دحل لخدأ
 - Interval(Second): نكمي يذال ينمزلال لصاللال لخدأ، اقبس م اءنيوك مت يتال "لئاسرلا دء" ءم لءملا ىل اذانتسا
- ءد دعمال لصاللال لئاسر نم ءتباث ءومجم يقلا هءف syslog.

ءنمزلال لصاللال/لئاسرلا دء وه syslog ل دعم



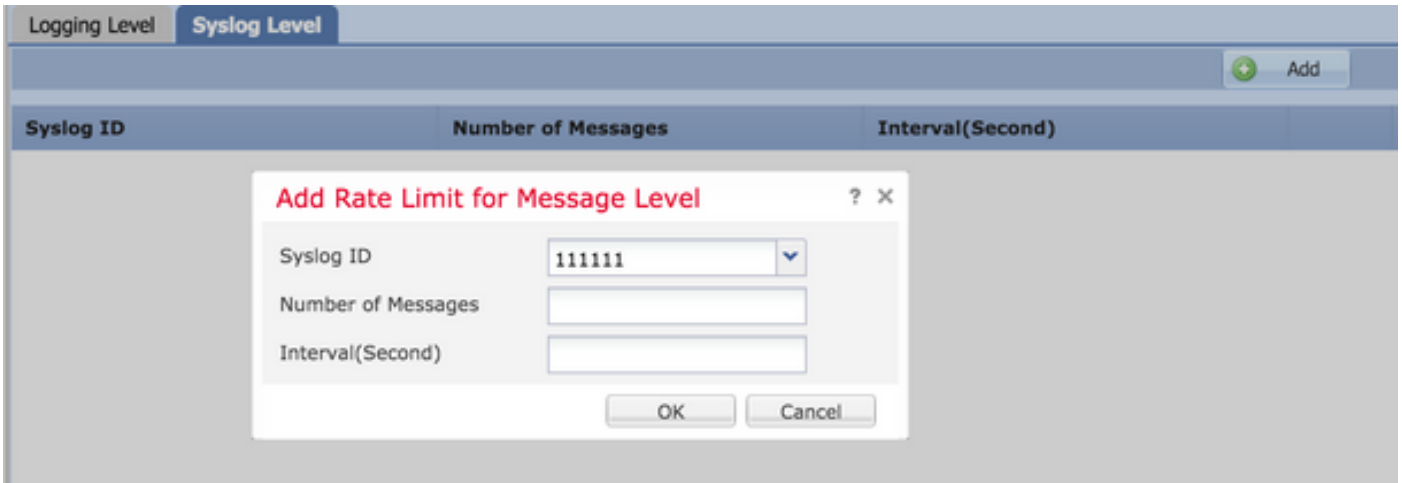
The screenshot shows a web interface with two tabs: 'Logging Level' and 'Syslog Level'. An 'Add' button is in the top right. Below the tabs is a table with columns for 'Logging Level', 'Number of Messages', and 'Interval(Second)'. A modal dialog box is open over the table, titled 'Add Rate Limit for Syslog Logging Level'. The dialog has a dropdown for 'Logging Level' set to '0 - emergencies', and empty input fields for 'Number of Messages' and 'Interval(Second)'. 'OK' and 'Cancel' buttons are at the bottom of the dialog.

ليجستال يوتسم نيوك تظفلل OK رقنا

Add. قوف رقناو Logging Level رتخأ، ليجستال يوتسم ىل اذنتسم ل دعمال دح نيكم تل

- Syslog ID: ءلدسنم Syslog ID ءم اقلال نم. اذرف لكشب Syslog لئاسر فيءرءل Syslog تاءرءم اءءءسا متي Syslog ID
 - Number of Messages: ءد دعمال ءنمزلال ءرتفلال لال خ اءقلا متيس يتال syslog لئاسر دءل صقأال دحل لخدأ
 - Interval(Second): نكمي يذال ينمزلال لصاللال لخدأ، اقبس م اءنيوك مت يتال "لئاسرلا دء" ءم لءملا ىل اذانتسا
- ءد دعمال لصاللال لئاسر نم ءتباث ءومجم يقلا هءف syslog.

ءنمزلال لصاللال/لئاسرلا دء وه syslog ل دعم



ليكشت يوتسم syslog ال تذقنأ in order to OK تقطقط

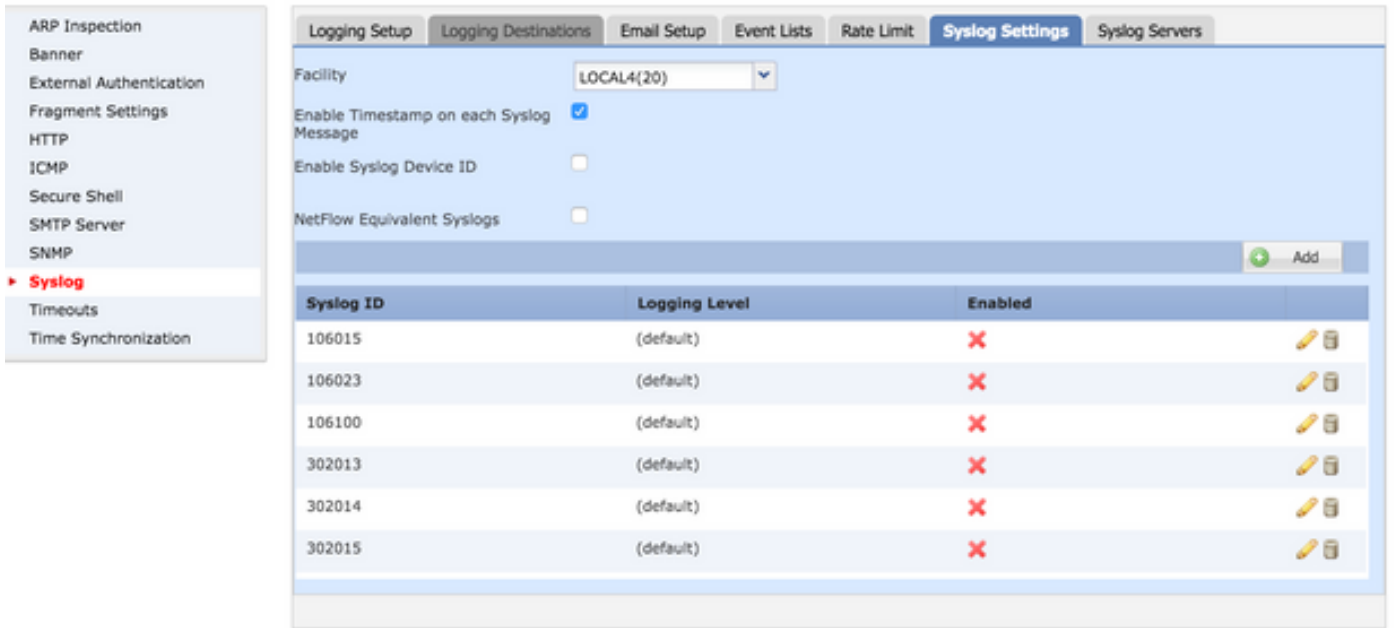
عدبل Deploy رقناو، تاريخيغتللا قيبطت ديرت شيح FTD زاه رتخأ Deploy، ديرت ام رتخأ. ياساسألماظنللا دادع| ظفحل Save رقنا ياساسألماظنللا دادع| رشن

Syslog تادادع|

لائسري في ينمزللا عباطلا نيمضت اضيأ كنكمي. Syslog لئاسري في Facility ميق نيوكت نيمضت Syslog تادادع| حيتت syslog. مداخل ةصاخلا يرخالأ تاملعملاول لجلسلا

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

- Facility: لئاسرلا عم لماعتلا نكمي. ةلاسرلا ليجستب موقوي يذلا جم انربلا عون ديدحتل قفرم دوكم ادختسا متي: Facility. ةأشنملا ةميقرتخأ، ةلدسنملا Facility ةمئاقلا نم. فل تخم لكشب ةفل تخملا قفارملا تاذ
- Enable Timestamp on each Syslog Message: نيمضتل رايتخالأ Enable Timestamp on each Syslog Message ةناخ دح Syslog لئاسري في ينمزللا عباطلا
- Enable Syslog Device ID: ريغ syslog لئاسري في زاهجلا فرعم نيمضتل رايتخالأ Enable Syslog Device ID ةناخ دح. راعش قيسنتب
- Netflow Equivalent Syslogs: نأ نكمي. NetFlow ل ةئفكلملا Syslog لئاسرلا رايتخالأ Netflow Equivalent Syslogs ةناخ دح. زاهجال عادأ يلع رثؤي
- رايتخالأ Syslog ID/ Logging Level ع برم ددحو Add رقنا، فياضالا syslog فرعم ديدحتل: ددحم syslog فرعم ةفاضلا



عدبل **Deploy** رقناو، تاريغيغتال قيبطت ديتر شيح FTD زاه رتخ **Deploy**، ديتر ام رتخ. ياساسال اماظنل دادع | ظفح **Save** رقنا ياساسال اماظنل دادع | رشن

ليحلجل ليجستال نيوكت

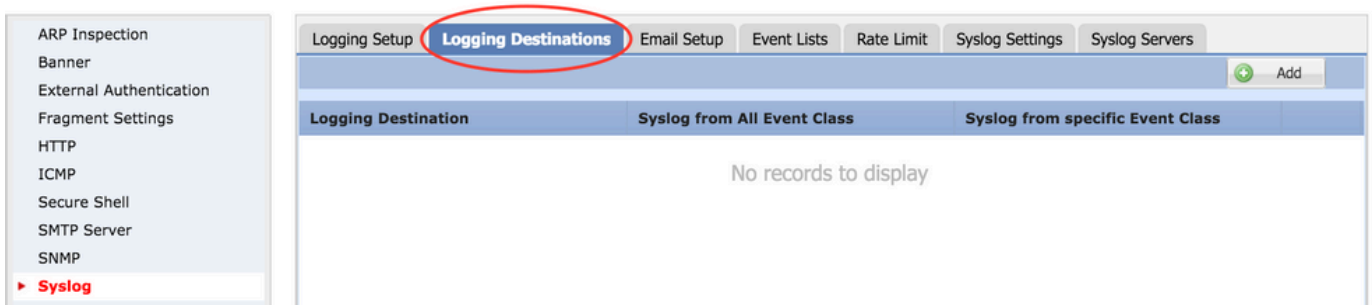
ةددم تاهجو ىل ليجستال نيوكتل ليجستال ةهجو مسق مادختسا نكمي

ي: ةرفوتملا ةيلخادلا ليجستال تاهجو

- (ليجستال اتقؤم نزملا) يلخادلا ليجستال اتقؤملا نزملا ي ةدوجوملا تالجسلا: يلخادلا اتقؤملا نزملا
- (ليجستال مكحت ةدحو) مكحتال ةدحو ىل تالجسلا لسري: مكحتال ةدحو
- (ةيرطال ةبقارملا) SSH تاسلج ىل Syslog ليجستال: SSH تاسلج

ليحلجل ليجستال نيوكتل تاوطخ ثالث كانه

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



الخطا 2. رقنا **Add** ددم ليجستال ةيفصت لماع ةفاضال **logging destination**.

وأمكن حث دمج أو إيقاف تشغيل أو تغيير إعدادات **Logging Destination** قائمة المصادق من قبل طم المايكروستريت: لجستلة هجوتاسلج SSH.

من قائمة وجمه هه شادأل تائف نإف، اقبس هفصومت امكو. شح ةئف رتخأ، ةلدسنم ال **Event Class** قائمة المصادق من: شحل ةئف قرتال هه شحل تائف ديدحت نكمي. تازيم السفن لثمت يتل syslogs:

- Filter on Severity: Syslogs ةروطخ إل اذانتسا شادأل تائف ةيفصت لماع.
- User Event List: ةصصم ال شادأل تائف عم (اقباس هفصومت) ةدحم شادأ مئوق عاشن ني لوؤس مل نكمي: م سقلا اذ هه عجارم هه ةصخال.
- Disable Logging: لجستلة يوتسم و ةراتخم ال لجستلة هجول لوخدل لجستل ليطعتل راخال اذ مدختسأ.

7 إل (ئراوطل تالاح) 0 من وه لجستلة يوتسم قاطن. ةلدسنم ال قائمة المصادق من لجستلة يوتسم رتخأ: لجستلة يوتسم (ءاطأل احيصت).

Add Logging Filter

Logging Destination: Internal Buffer

Event Class: Filter on Severity

Syslog Severity: emergencies

Event Class	Syslog Severity
Filter on Severity	
Use Event List	
Disable Logging	

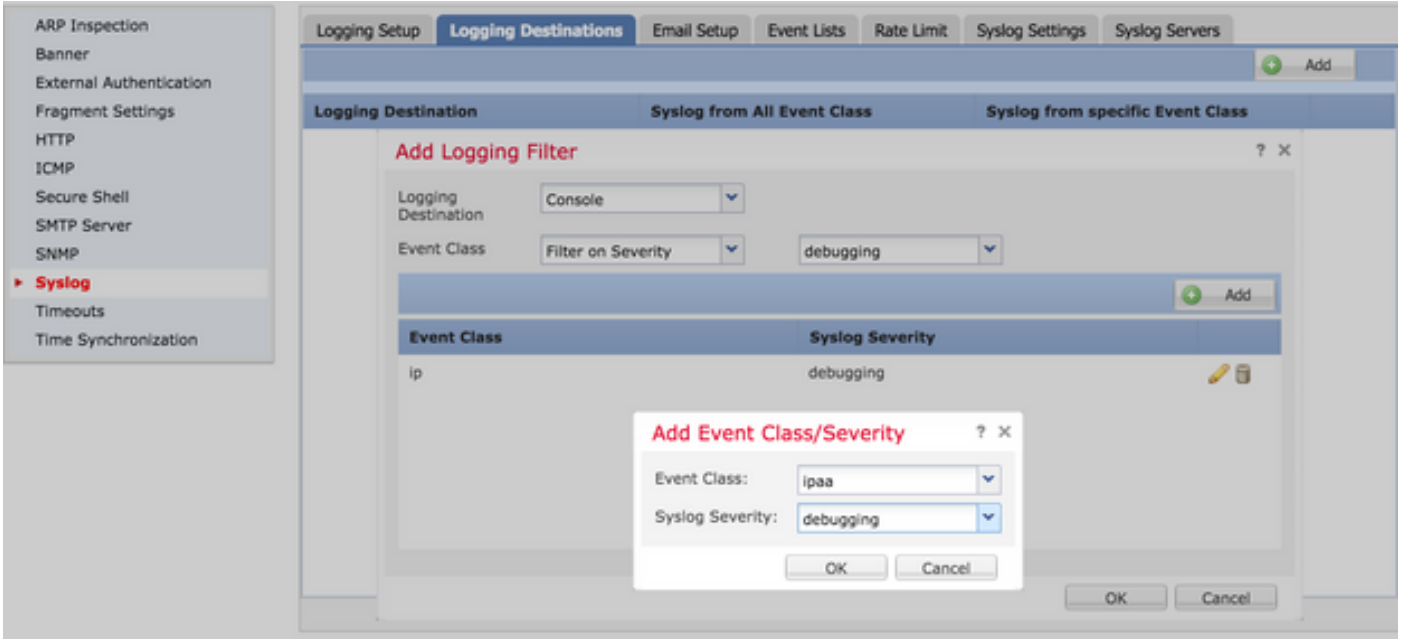
No records to display

OK Cancel

Add قوف رقنا، اذ لجستلة ةيفصت لماع إل ةلصفنم شح ةئف ةفاضل 3. ةوطخل

Event Class: ةلدسنم ال **Event Class** قائمة المصادق من "شحل ةئف" رتخأ.

Syslog Severity: ةلدسنم ال **Syslog Severity** قائمة المصادق من Syslog ةروطخ رتخأ.



ةددم ليجست ةهول ةيفصتلا لماع ةفاضال ةيفصتلا لماع نيوكت درجم OK رقا

رشن عدبل Deploy رقاو، تاريغتلا قيبطت ديرت شيح FTD زاغ رقا، Deploy رقا. ياسال ماظنلا دادع لظاح Save رقا ياسال ماظنلا دادع

يجراخل ليجستلا نيوكت

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

هذو جيراخل ليجستلا عاونأ FTD معدو

- دعب نع Syslog مداخ لىا تالجسلا لسري Syslog مداخ.
- ةمئالم كجراخل لىا تالجسلا لسري: SNMP ةمئالم.
- اقبس مهنوكت مت ديرت ليجستل مداخ مادختساب نيورتكلا لىا ديرت ربق تالجسلا لسري: نيورتكلا لىا ديرت.

م تي يذلا ليجستلا عون ليجستلا تاهو ديدحت دحي. هسفن وه يلخادلا ليجستلاو جيراخل لىا ليجستلا صاخلا نيوكتلا ديعبلا مداخ لىا "ةصصخملا ثادحل" مئوق لىا ادانتسا "ثادحل تائف" نيوكت نكمم نم. هذيفنت

دعب نع Syslog مداخ

FTD لوكوتورب نم دعب نع اهنينختو تالجسلا لىا لىا لىا Syslog مداوخ نيوكت نكممي

ةديعبلا syslog مداوخ نيوكتل تاوطخ ثالث كانه

1. ةوطخلا Device > Platform Setting > Threat Defense Policy > Syslog > Syslog Servers

2. ةوطخلا syslog مداخ ةلصلا تاذمة لىا نيوكت ب مق.

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. سيسألل ماظنل دادع| ظفحل **Save** رقن ا سيسألل ماظنل دادع|

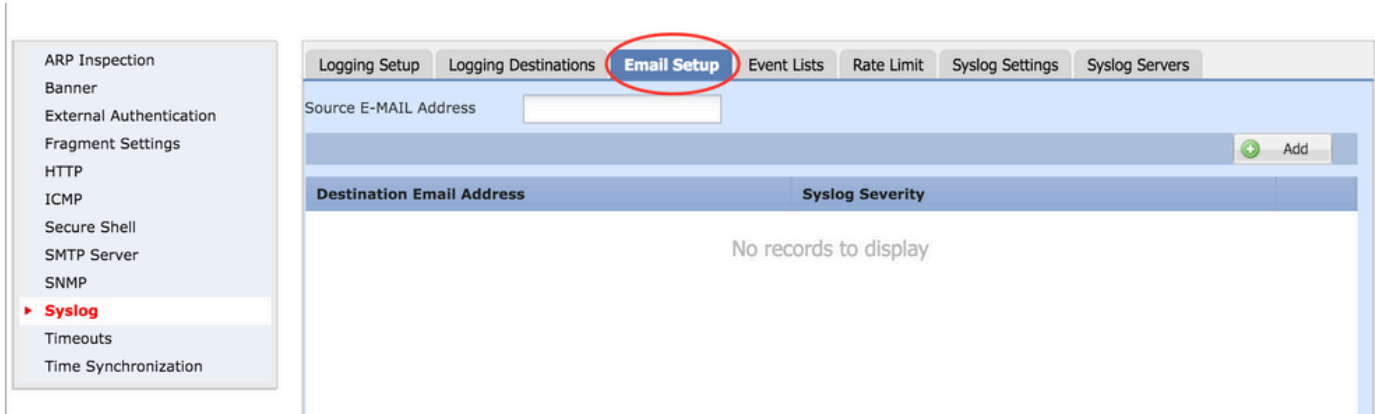
ليجستلل ينورتكللال ديربل دادع|

يف طقف ليجستة جوك ينورتكللال ديربل مادختس| نكمي. ددحم ينورتكللال ديرب ناونع الى syslog لاسراب كل FTD حمسي لعلفالاب ينورتكللال ديربل ليجرت مداخ نيوكتة للاح.

syslogs ل دادع| لجمع ينورتكللال ديرب لكشي نأ steps نانث| كانه

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

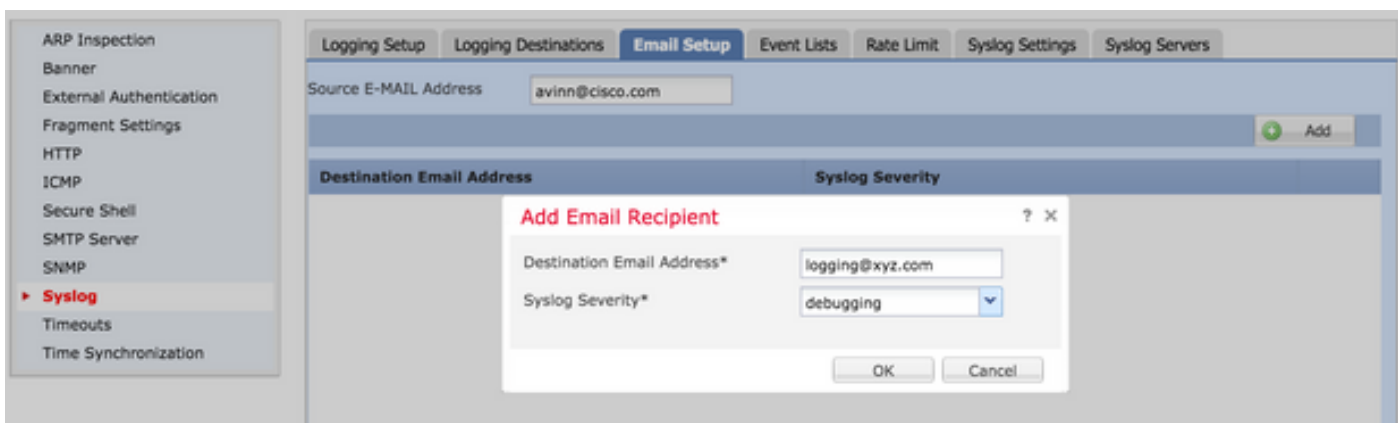
نم لاسرملل ينورتكللال ديربل لئاسر ةفاك الى لعل رهظي يذل رصملا ينورتكللال ديربل ناونع لخدأ: Source E-MAIL Address: syslogs لعل يوتحت يتلاو FTD



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 ترقوط.

رشن عدبل Deploy رقناو، تاريغتلا قيبطت ديرت شيح FTD زاغ رتخأ، Deploy رتخأ. ياساسألا ماظنلا دادعإ ظفح Save رقنا ياساسألا ماظنلا دادعإ.

ةحصلا نم ققحتلا

نيوكتلا اذه ةحص نم ققحتلل ءارجإ آيلاج دجوي ال.

اهالصال ءاطخألا فاشكتسا

اهالصال نيوكتلا ءاطخأ فاشكتسال اهمادختسا كنك م ي تامولعم مسقلا اذه رفوي.

- system لخدأو، FTD ةرادإ ةهجاو ىلا لوخدلا ليحس تب مق FTD نم رماوألا رطس ةهجاو يف FTD syslog نيوكت نم ققحت ةصيصيخشثلا رماوألا 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 - تادنت سمل او ينقتال معدل](#)

ةمچرتل هذه لوج

ةللأل تاي نقتل نمة ومة مادختساب دن تسمل اذة Cisco تمةرت
ملاعلاء انء مء مء نمة دختسمل معد ىوتحم مء دقتل ةر شبل او
امك ةق قء نوك ت نل ةللأل ةمچرت لصف أن ةظحال مء ءرء. ةصاأل مء تءل ب
Cisco ةللخت. فرتحم مچرت مءم دقء ةللأل ةل فارتحال ةمچرتل عم لاعل او
ىل إأمءءاد ءوچرلاب ةصوءو تامچرتل هذه ةقء نء اهءل وئس م Cisco
Systems (رفوتم طبارل) ةل صأل ةل ءل ءن إل دن تسمل