

انثأ اءوسلا ةمئاقلا يف IP ءارءا نيوكت ASDM لالء نم Cisco نم نامألا ءاكء ماءءسا (ءبرملا لءاء ةراءالا)

ءاىوءءملا

[ءمءملا](#)

[ءيساسألا ءابلءملا](#)

[ءابلءملا](#)

[ءمءءسملا ءانوءملا](#)

[ءيساسأءامولءم](#)

[نامألا ءامولءم ءءم ءمء ءمء ءمء](#)

[ءيملاءلا ءاضيبلا مءاوءلا ءملاءلا ءءمءملا ءمءمءملا ءمءمءملا ءمءمءملا](#)

[ءءوسلا ءمءمءملا ءمءمءملا ءمءمءملا ءمءمءملا](#)

[نامألا ءامولءم نيوكت](#)

[رشنلا ءمءمءملا ءمءمءملا ءمءمءملا](#)

[ءمءمءملا ءمءمءملا ءمءمءملا](#)

[ءءمءملا ءمءمءملا](#)

[ءءمءملا ءمءمءملا ءمءمءملا](#)

[ءمءمءملا ءمءمءملا](#)

ءمءملا

IP ل ءءوسلا ءمءمءملا نيوكتو Cisco نم نامألا ءامولءم/IP ءمءمءملا ءمءمءملا ءمءمءملا ءمءمءملا (رءءمءملا).
ءمءمءملا ءمءمءملا IP ءمءمءملا ءمءمءملا ءمءمءملا ءمءمءملا ءمءمءملا.

ءيساسألا ءابلءملا

ءابلءملا

ءمءمءملا ءمءمءملا ءمءمءملا ءمءمءملا ءمءمءملا:

- لءمءملا نامألا ءمءمءملا (ASA) ءمءمءملا لءمءملا نامألا ءمءمءملا ءمءمءملا (ءمءمءملا)
- FirePOWER نامألا ءمءمءملا ءمءمءملا

ءمءمءملا ءمءمءملا ءمءمءملا ءمءمءملا: ءمءمءملا

ءمءمءملا ءانوءملا

ءمءمءملا ءمءمءملا ءمءمءملا ءمءمءملا ءمءمءملا ءمءمءملا:

- ASA FirePOWER (ASA 5506X/5506H-X/5506W-X، ASA 5508-X، ASA

يلع أو 5.4.1 رادصلال لغشت يتل (5516-X

- ASA FirePOWER (ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X) ةيطمنللا ةدحوللا

يلعألا تارادصلال او 6.0.0 رادصلال لغشت يتل

ةصاخ ةيلمعم ةئيبي ف ةدوحووملا ةزهجال نم دنتسمللا اذ ف ةدراوللا تامولعمللا ءاشنل م تناك اذ (يضا رتفا) حوسم نيوكتب دنتسمللا اذ ف ةمدختسمللا ةزهجاللا عيمج تادب رما يال لم تحملا ريثاتلل كمهف نم دكاتف ، ةرشابم كتكتبش

ةيساسأ تامولعم

م IP نيوانعل مظتنم لكشب ةثدحم تاعومجم ةدع نم Cisco نم نامألا تاربابم فلأتت Cisco TALOS قيرف ددحي Cisco Talos قيرف ةطساوب ةئيس ةعمس تاذ اهنأ نم ققحتللا جماربال او IP مزح لثم هذه IP نيوانع نم راض طاشن ي ءاشنل م اذا ةضفخنملا ةعمسللا كلذ يلا امو عا دخل تامجهو ةراضللا

و Bogon و نيجمهمل تانايب ةدعاق Cisco IP Security Intelligence نامأ تامولعم زجوم عبتتتي و Spam و Response و Phishing و Open_relay و Open_proxy و ExploitKit و DGA و CnC و Bots و IP ناوعل صصخم بيو زجوم ءاشنل راخي FirePOWER ةيطمنللا ةدحوللا رفوت Suspicious. ةعمسللا ضفخنم

نامألا تامولعم زجوم يلع ةماع ةرظن

اهفني نصت نكمي يتل IP نيوانع تاعومجم عون لوح ةيفاضللا تامولعمللا ضعبي لي امي ف نامألا ءاكذ ف ةفلتخم تائفك

ةلواحم و افعضلا طاقن نع اثحب رارمتساب اهحسم متي يتل IP نيوانع ةعومجم : نيجمهمللا سارخا ةمظنأ لالغتسا

يا ةمجهمب موقت و اراضللا جماربالا رشن لواح يتل IP نيوانع ةعومجم : ةراضللا جماربالا طشن لكشب اهترايب موقبي صخش

عا دخل طشن لكشب لواح يتللا ةفيضملا تائيبيلا نم ةعومجم : لاي تحاللا ديصتلا رورملا تاملك و نيمدختسمللا ءامسأ لثم ةيرس تامولعم لاخ دل نيئيئا هالنلا نيمدختسمللا

لائسار لاسرل ردصمك اهديحت مت يتللا ةفيضملا تائيبيلا نم ةعومجم : يئاوشعللا ديربالا يئاوشعللا ينورتكللا لاللا ديربالا

زاهج اهيف مكحتيو ، ام ةكبش ي ف طاشن ب كراشت يتللا ةفيضملا ةزهجالا نم ةعومجم : توب فورعم توب ةكبش م كحت

BOTNET ةكبشل م كحت مداوخك اهديحت مت يتللا ةفيضملا تائيبيلا نم ةعومجم : CNC ةفورعم

بيولا تاييسكورب " ليغشتب ةفورعمللا ةفيضملا تائيبيلا نم ةعومجم : OpenProxy ةلوهجم بيو ضارعتسا تامدخ مي دقتو " ةحوتفملا

ديربالا ليحرت تامدخ مي دقتب ةفورعمللا ةفيضملا تائيبيلا نم ةعومجم : OpenRelay عا دخل او يئاوشعللا ديربالا ومجهام اهمدختسي يتللا لوهجملا ينورتكللا لاللا

ةكبشل جورخللا دقع تامدخ مي دقتب ةفورعمللا ةفيضملا تائيبيلا نم ةعومجم : TorExitNode

Tor. ةيوهال لوجم

رورم ةكرح لسرت اهنكلو ةصصخملا ريغ IP نيوانع ةعومجم **Bogon**.

طشنل شحبلا ديقي يتلاو ابيرم اطاشن رهظت يتلا IP نيوانع ةعومجم **بيري**.

كولسلاب مايقلا اناثا رركتم لكشب اهتظالم مت يتلا IP نيوانع نم ةعومجم **باجتسالا** راضلا و ابيرملا.

ةيملاعال اءوسلا ةمئاقلا لىل ايوذي IP نيوانع ةفاضل ةيملاعال اءاضيبلا مءاوخلاو

امءنع ةيملاعال اءوسلا ةمئاقلا لىل ةنيعم IP نيوانع ةفاضل **FirePOWER** ءءوكل ءمست تنك اذا **Global-Whitelist** لىل IP نيوانع ةفاضل اءىل نكمي. راض طاشن نم ءزء اءنا فرعت ةمئاقلا لىل IP نيوانع ةطساوب اءرظء مءى ةنيعم IP نيوانع لىل رورملا ةكرحب ءامسلا ءيرت زيء لءءى هءا **Global-BlackList/Global-Whitelist** لىل IP ناوع اءىل ةفاضل تمق اذا. اءوسلا ةسايسلا قيبطت لىل ءءءال نوء روفلا لىل ءىفءنءلا.

ASA > ةبقارملا لىل لقتنا **Global-BlackList/ Global-Whitelist** لىل IP ناوع ةفاضل لءا نم ءءو لاصءالا ءاءءا لىل سواملا كىرءءب مق **FirePOWER Monitoring > Real Time Eventing** ءءو رءلا رىرء لىل صافءلا ضرء.

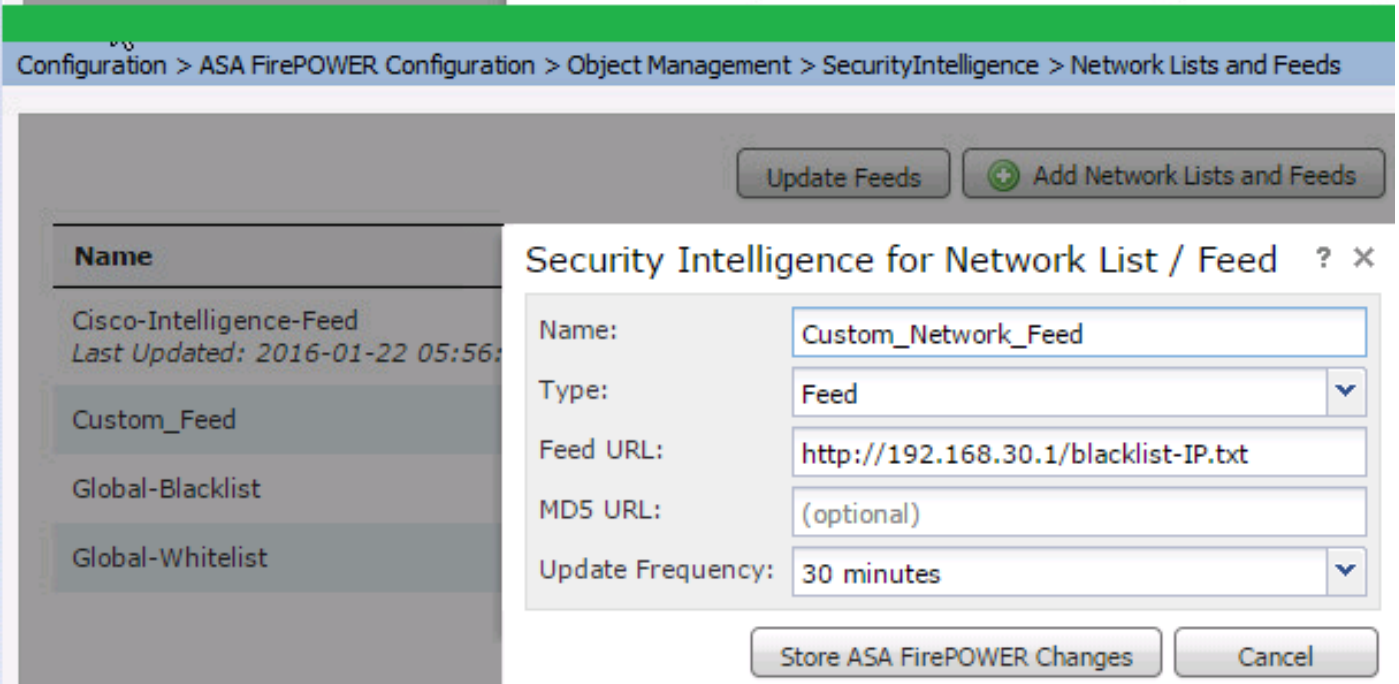
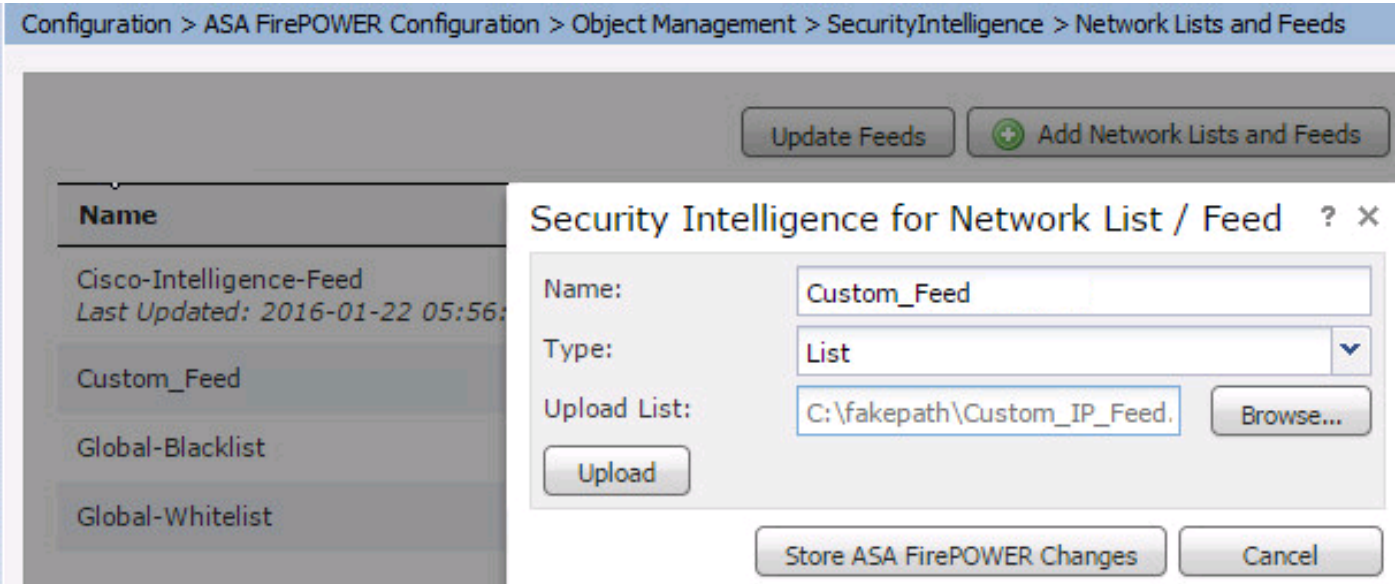
قوف رقنا **global-blackList/ global-whitelist** لىل ءءءو و اءصملا لىل IP ناوع اءىل ةفاضل كءمى وه امك، ءلباقملا ةمئاقلا لىل IP ناوع ةفاضل **WhiteList Now/BlackList** ءءو رءلا رىرء ءءو لىل صافءلا ضرء.

ةلدسنم لةمئاق ل ن م رايخل ل ب و زوم دح :عون ل

ةدح و ه ب لصت ن أ ب جي يذ ل مداخل ب صا ل ل URL ناون ع دح :ب يول ا زوم URL ه ل ب يول ا زوم ل يزن ت و ة ي ط م ن ل FirePOWER

زوم ل ل URL ناون ع راس م ن م ق قحت ل ل ة ئزجت ل ة م ي ق دح : MD5 ل URL ناون ع

URL ب ي و زوم مداخل م اظن ل ه ي ف لصت ي يذ ل ي ن م زل ل صا ف ل دح :ث ي دح ت ل رار ك ت

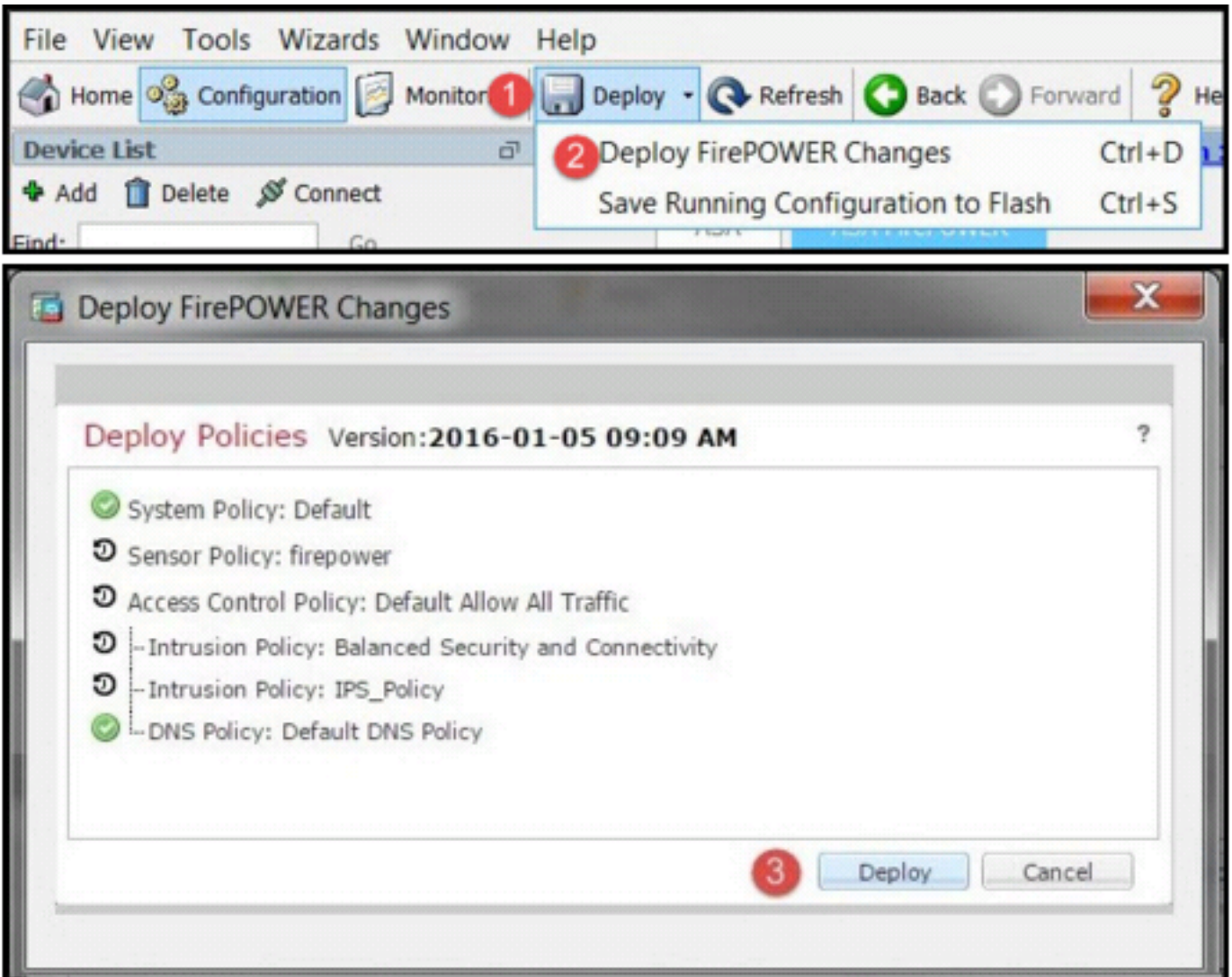


ن ا م ا ل ا ت ا م و ل ع م ن ي و ك ت

> تاس ا ي س ل ل > ASA Firepower Configuration > ن ي و ك ت ل ل ا ل ل ق ت ن ا ، ن ا م ا ل ا ء ا ك ذ ن ي و ك ت ل ن ا م ا ل ا ت ا م و ل ع م ب ي و ب ت ل ل ة م ا ل ع دح ، ل و ص و ل ا ي ف م ك ح ت ل ل ة س ا ي س

ر ط ح / ح ا م س ل ل Whitelist/ BlackList دوم ع ا ل ل ق ت ن ا و ، ح ا ت م ل ة ك ب ش ل ل ن ئ ا ك ن م ب ي و ل ا زوم ر ت خ ا راض ل ل IP ناون ع ب ل اص ت ل ا

ةرو ص ل ل ا ي ف دح م و ه ا م ك ل ي ج س ت ل ل ن ي ك م ت و ة ن و ق ي ا ل ر ق ن ك ن ك م ي

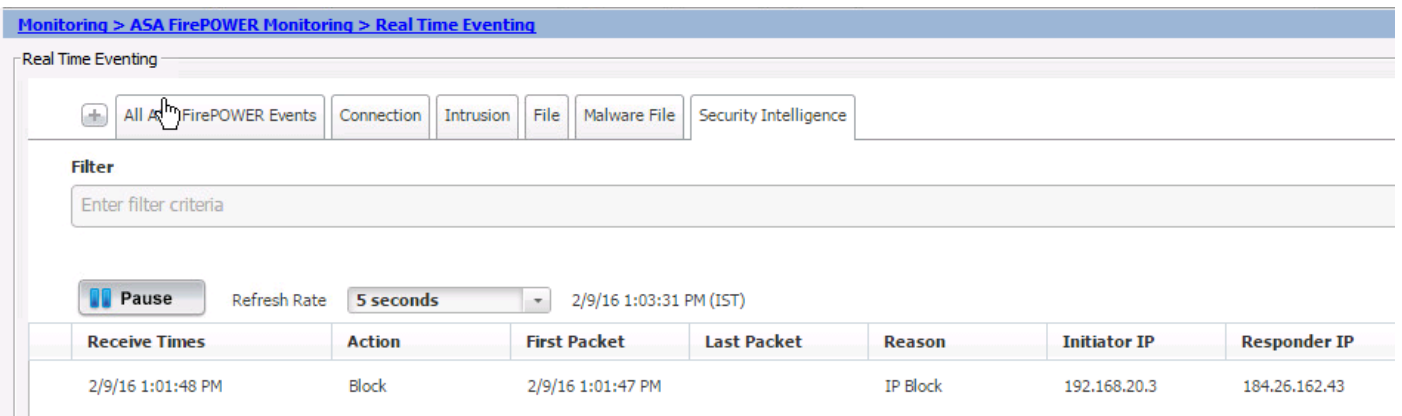


ASA FirePOWER تاريخي غت قيبطت قوف رقتل لكمزلي، رعشتسما لىلع لوصولت سايس قيبطت، 5.4.x رادصالا يف: ؤظالم

نيوكتلا تاريخي غت قيبطت ؤمهمل لاكمك بجي هنا نم دكات. ؤمهمل ؤلاح > ASA FirePOWER ؤبقارم > ؤبقارمدا لىل لقتنا: ؤظالم

ينمألا ؤاكذلا ؤادحأ ؤبقارم

ASA ؤبقارم > ؤبقارمدا لىل لقتنا، FirePOWER ؤدحو ؤطساوب نامألا ؤاكذ ؤدهاشمل كلذ يدؤيس. نامألا تامولعم بيوبتلا ؤمالع دح. لىلعفلا تقولا يف قيقدتلا > FirePOWER ؤروسلا يف حضورم وه امك ؤادحألا راهظا لىل:



ةحصلا نم ققحتلا









نيوكتلا اذه ةحص نم ققحتلل ءارجا آيلا ح دجوي ال

اهحالصوا ءاطخالا فاشكتسا

ASA نيوكت > نيوكتلا ىلإ لقتنا ، ةثدحم ةيكدذلا نامالا تامولعم تاميقتل نأ نامضل مت يذلا تقولا ددحو بيولا زجومو ةكبشلا مئاق > نامالا ءاكذ > نئاكل ءراد | FirePOWER > بيولا زجوم شيدحت راركت طبضل ريحت رز رايتخا كنكمي . ءرم رخا هي ف بيولا زجوم شيدحت

Configuration > ASA FirePOWER Configuration > Object Management > SecurityIntelligence > Network Lists and Feeds

Update Feeds Add Network Lists and Feeds Filter

Name	Type	
Cisco-Intelligence-Feed Last Updated: 2016-02-08 10:03:14	Feed	 
Custom_Feed	Feed	 
Global-Blacklist	List	 
Global-Whitelist	List	 

حاجنب لوصولاب مكحتلا جهن رشن لامتك نم دكأت

ال مأ ءلطم رورملا ءكرح تناك اذا ام ءفرعمل ةينمألا ةيتارابختسالا تامولعمل بقار

ءلص تاذ تامولعم

- [Cisco ASA FirePOWER Module](#) ةيظمنلا ءدحولل عيررسلا ءدبلا ليلد
- [Cisco Systems](#) - تادنستسمل او ينقتلا معدلا

ةمچرتل هذه لوج

ةللأل تاي نقتل نم ةومچم مادختساب دن تسمل اذہ Cisco تچرت
ملاعلاء انءمچي فني مدختسمل معدى وتحم مي دقتل ةيرشبلاو
امك ةقيقد نوك تنل ةللأل ةمچرت لصف أن ةظحال مچري. ةصاخلا مهتغب
Cisco يلخت. فرتحم مچرت مامدقي يتل ةيفارتحال ةمچرتل عم لالحل وه
ىلإ أمئاد عوچرلاب ي صؤت وتامچرتل هذه ةقد نع اهتيلوئسم Cisco
Systems (رفوتم طبارلا) ي لصلأل يزي لچنل دن تسمل