

# مماظن ىل ع LDAP ةقداصم نئاك نىوكا FireSIGHT

## المحاااا

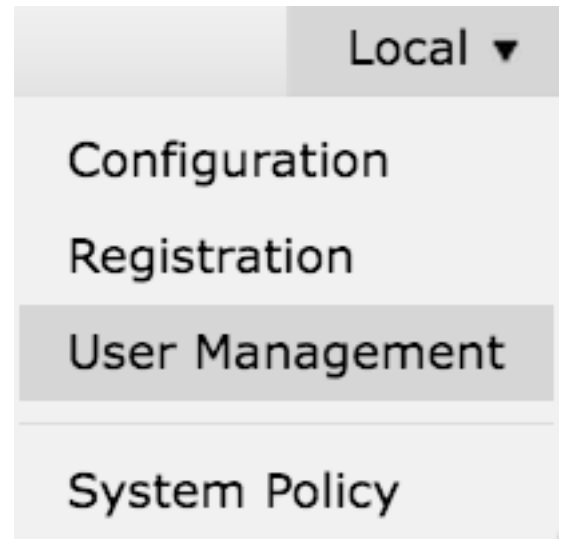
[المقماة](#)  
[اكويا كائا مصادقا LDAP](#)  
[مساا ذو صلا](#)

## المقماة

كائاا المصادقا هى اوصيفاا ااام لخواام المصادقا اارااا، اااوا على إعاااا الاااا وإعاااا مرشأ المصادقا لئاك اخواام. مماكك إنااا كائاا المصادقا وإارااا وحاااا فى مركا إاراة FireSIGHT. اواأ هذا المسااا كىفاة اكويا كائا مصادقا LDAP على نظام FireSIGHT.

## اكويا كائا مصادقا LDAP

1. ااااا الاااا إلى واااة مسااا الواب ااااا بمركا إاراة FireSIGHT.
2. ااااا إلى النظام < مالا < إاراة المساااا.



اااا علامة ااااا مصادقا ااااا الاااا.



انقر على إنااا كائا مصادقا.



## Create Authentication Object

3. حدد أسلوب مصادقة ونوع خادم.

- أسلوب المصادقة: LDAP
- الاسم: <اسم كائن المصادقة>
- نوع الخادم: MS Active Directory

ملاحظة: الحقول المميزة بالعلامات النجمية (\*) مطلوبة.

### Authentication Object

Authentication Method

LDAP

Name \*

Description

Server Type

MS Active Directory

4. حدد اسم مضيف خادم النسخ الاحتياطي الأساسي واسم مضيف خادم النسخ الاحتياطي أو عنوان IP. خادم النسخ الاحتياطي إختياري. ومع ذلك، يمكن استخدام أي وحدة تحكم بالمجال ضمن المجال نفسه كخادم نسخ إحتياطي.

ملاحظة: على الرغم من أن منفذ LDAP هو الإعداد الافتراضي للمنفذ 389، إلا أنه يمكنك استخدام رقم منفذ غير قياسي يقوم خادم LDAP بالإصغاء إليه.

5. حدد المعلومات الخاصة ب LDAP كما هو موضح أدناه:

تلميح: يجب تحديد سمات المستخدم والمجموعة و OU قبل تكوين المعلومات الخاصة ب LDAP. [قراءة هذا المستند](#) للتعرف على سمات كائن LDAP ل Active Directory لتكوين كائن المصادقة.

- شبكة DN الأساسية - المجال أو شبكة DN الخاصة
  - عامل التصفية الأساسي - شبكة DN الخاصة بالمجموعة التي ينتمي إليها المستخدمون.
  - اسم المستخدم - حساب التمثيل للتيار المستمر
  - كلمة السر: <password>
  - تأكيد كلمة المرور: <password>
- الخيارات المتقدمة:

- التشفير: SSL أو TLS أو لا شيء
- مسار تحميل شهادة SSL: تحميل شهادة CA (إختياري)
- قالب اسم المستخدم: %s
- المهلة (بالثواني): 30

**LDAP-Specific Parameters**

Base DN \*   ex. dc=sourcefire,dc=com

Base Filter  ex. (cn=jsmith), (&(cn=jsmith), (&(cn=bsmith)(cn=csmith\*)))

User Name \*  ex. cn=jsmith,dc=sourcefire,dc=com

Password \*

Confirm Password \*

Show Advanced Options ▼

Encryption  SSL  TLS  None

SSL Certificate Upload Path   ex. PEM Format (base64 encoded version of DER)

User Name Template  ex. cn=%s,dc=sourcefire,dc=com

Timeout (Seconds)

في إعداد نهج أمان المجال الخاص ب AD، إذا تم تعيين متطلبات توقيع خادم LDAP على يتطلب التوقيع، فيجب استخدام SSL أو TLS.

### متطلبات توقيع خادم LDAP

- none: توقيع البيانات غير مطلوب للربط مع الخادم. إذا طلب العميل توقيع البيانات، سيقوم الخادم بدعمه.
- يتطلب التوقيع: ما لم يكن TLS\SSL قيد الاستخدام، يجب التفاوض بشأن خيار توقيع بيانات LDAP.

ملاحظة: لا يلزم الحصول على شهادة من جانب العميل أو شهادة CA (شهادة CA) لنقاط الوصول من المستوى الأدنى (LDAP). ومع ذلك، سيكون هذا مستوى إضافي من تأمين شهادة CA يتم تحميله إلى كائن المصادقة.

6. تحديد تعيين السمة

- سمة الوصول إلى واجهة المستخدم: sAMAccountName
- سمة Shell Access: sAMAccountName

**Attribute Mapping**

UI Access Attribute \*

Shell Access Attribute \*

تلميح: إذا واجهت رسالة "مستخدمين غير مدعومين" في إخراج الاختبار، قم بتغيير سمة الوصول إلى واجهة المستخدم إلى userPrincipalName وتأكد من تعيين قالب اسم المستخدم على s%.

Unsupported Admin Users

The following administrator shell access users (3) were found with this filter but are invalid because their format is not supported for this appliance:

-----

secadmin1 , secadmin2 , secadmin3

Unsupported Users

The following users (3) were found with this filter but are invalid because their format is not supported for this appliance:

-----

secadmin1 , secadmin2 , secadmin3

\*Required Field

7. تكوين أدوار الوصول المتحكم بها بواسطة المجموعة

في `ldp.exe`، استعرض كل مجموعة وانسخ رقم DN للمجموعة المطابقة إلى كائن المصادقة كما هو موضح أدناه:

• `<Group Name> Group DN: <group dn>`

• **سمة عضو المجموعة:** يجب أن يكون دائما عضوا

مثال:

• **مسؤول مجموعة** `CN=DC، CN=DC، DN: CN=DC، DC، DC=VirtualLab، DC=محلي`

• **سمة عضو المجموعة:** عضو

تحتوي مجموعة أمان AD على سمة **عضو** يتبعها DN الخاص بالمستخدمين الأعضاء. يشير الرقم السابق لسمة **العضو** إلى عدد المستخدمين الأعضاء.

```
3> member: CN=secadmin3,CN=Users,DC=VirtualLab,DC=local; CN=secadmin2,CN=Users,DC=VirtualLab,DC=local; CN=secadmin1,CN=Users,DC=VirtualLab,DC=local;
```

8. حدد نفس عامل التصفية الأساسي لعامل تصفية الوصول إلى Shell، أو حدد السمة `memberOf` كما هو موضح في الخطوة 5.

**عامل تصفية الوصول إلى group DN** (`Shell: (memberOf=`

على سبيل المثال،

**عامل تصفية الوصول إلى** `Shell: (memberOf=CN=Shell users.CN=Security`  
(`Groups.DC=VirtualLab,DC=local`)

9. حفظ كائن المصادقة وإجراء إختبار. تبدو نتيجة الإختبار الناجحة كما يلي:



## Info



### Administrator Shell Test:

3 administrator shell access users were found with this filter.

See Test Output for details.



## Info



### User Test:

3 users were found with this filter.

See Test Output for details.



## Success



Test Complete: You may enter a test user name to further verify your Base Filter parameter.

Admin Users

The following administrator shell access users (3) were found with this filter:

-----

secadmin1, secadmin2, secadmin3

Users

The following users (3) were found with this filter:

-----

secadmin1, secadmin2, secadmin3

\*Required Field

Save

Test

Cancel

10. بمجرد إجتياز كائن المصادقة للاختبار، قم بتمكين الكائن في نهج النظام وأعد تطبيق النهج على الجهاز الخاص بك.

## مستند ذو صلة

• [تعريف سمات كائن LDAP لخدمة Active Directory لتكوين كائن المصادقة](#)

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسمل اذ ه Cisco ت مچرت  
ملاعلاء ان ا عي مچ ي ف ن ي م دخت سمل ل معد ي و تح م مي دقت ل ة ي رش ب ل و  
امك ة ق ي قد ن و ك ت ن ل ة ي ل ة مچرت ل ض ف ا ن ا ة ظ حال م ي ج ر ي . ة ص ا خ ل م ه ت غ ل ب  
Cisco ي ل خ ت . ف ر ت ح م مچرت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة مچرت ل ا ع م ل ا ح ل ا و ه  
ي ل ا م ا د ع و ج ر ل ا ب ي ص و ت و ت ا مچرت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Cisco  
Systems (رف و ت م ط بار ل ا) ي ل ص ا ل ا ي ز ي ل ج ن ا ل ا دن تسمل ا