# دمج CUAC مع Microsoft AD

## المحتويات



## المقدمة

يصف هذا المستند الطريقة التي يعمل بها بروتوكول الوصول إلى الدليل خفيف الوزن (LDAP) بين وحدة تحكم الطلب التلقائي الموحدة (CUAC) من Cisco و (Microsoft Active Directory (AD والإجراءات التي يتم إستخدامها لدمج النظامين.

## المتطلبات الأساسية

### المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- CUCM
- كواك
- LDAP
- إعلان

### المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى الإصدار x.10 من CUAC.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

## معلومات أساسية

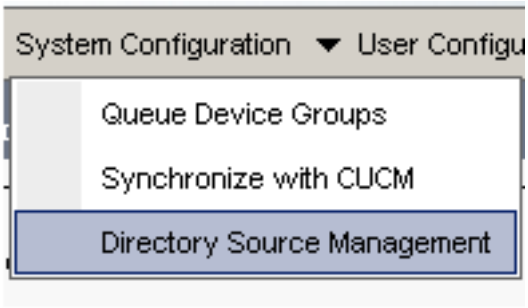
في إصدارات CUAC السابقة، يحصل الخادم على المستخدمين مباشرة من مدير الاتصالات الموحدة (CUCM) من Cisco من خلال الاستعلامات وعوامل التصفية المحددة مسبقا. مع إصدار CUAC Premium (CUACPE)، يسمح للمسؤولين بدمج واستيراد المستخدمين مباشرة من AD. ويمنح هذا الأمر المسؤولين مرونة لتنفيذ السمات والمرشحات التي يختارونها هم ومتطلباتهم الخاصة.

**ملاحظة**: تم الآن إستبدال CUACPE بالإصدار المتقدم من CUAC للإصدارات 10 والإصدارات اللاحقة.

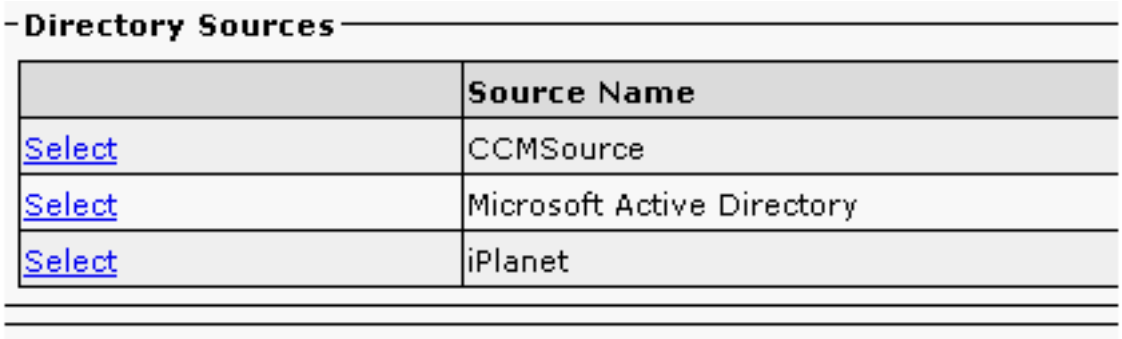
## دمج AD مع CUAC واستيراد المستخدمين من AD

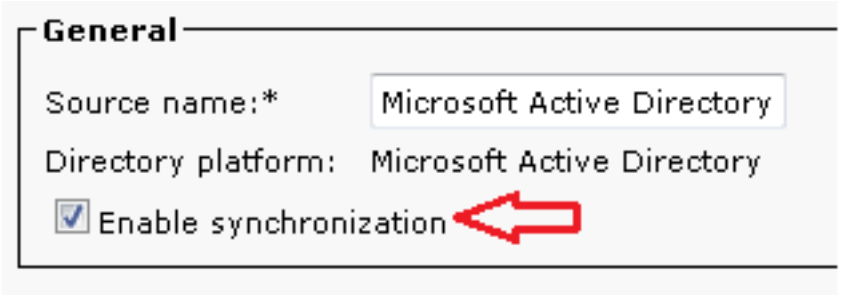
أكمل الخطوات التالية من أجل دمج CUAC مع الإعلان واستيراد مستخدمين من الإعلان:

1. تمكين مزامنة الدليل ل AD على CUAC.

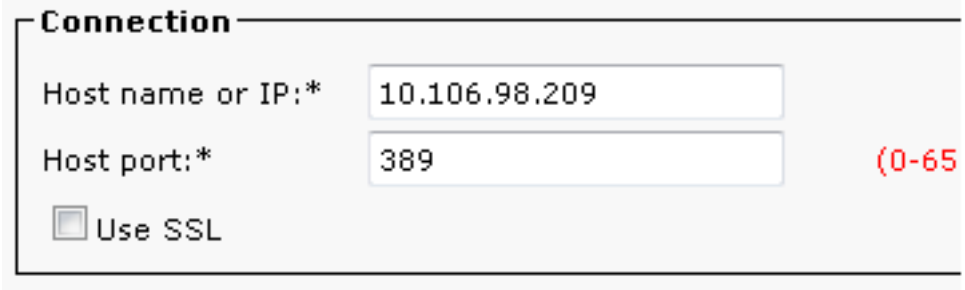



2. حدد **Microsoft Active Directory** وحدد خانة الاختيار **تمكين المزامنة**:

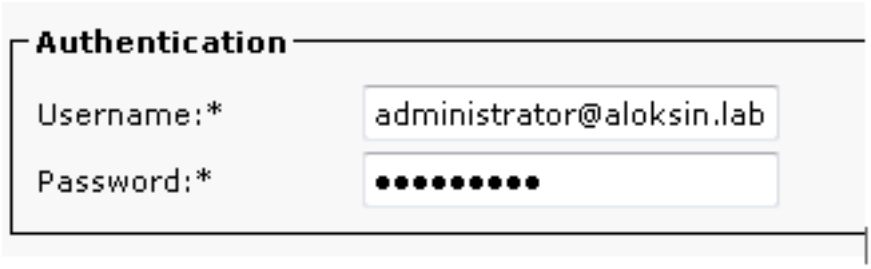


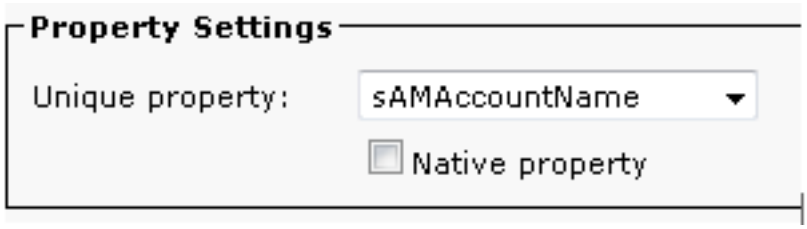

3. إدخال تفاصيل التكوين لخادم Active Directory:




على سبيل المثال، يتم إستخدام **administrator@aloksin.lab** للمصادقة:



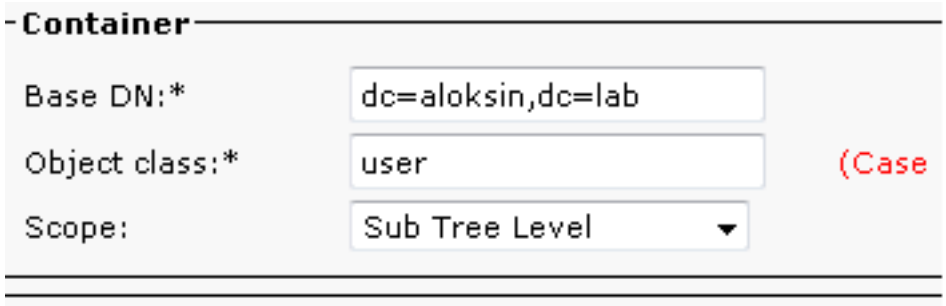

4. في قسم إعدادات الخاصية، أدخل تفاصيل التكوين للخاصية الفريدة، والتي تظهر بمجرد إدخال التفاصيل الأخرى وانقر فوق **حفظ**.




**ملاحظة**: هذه قيمة فريدة لكل مدخل في الإعلان. إذا كان هناك قيم مضاعفة، يسحب CUAC إدخالا واحدا فقط.

5. في قسم الحاوية، أدخل تفاصيل التكوين ل DN الأساسي، وهو نطاق بحث المستخدم في AD.

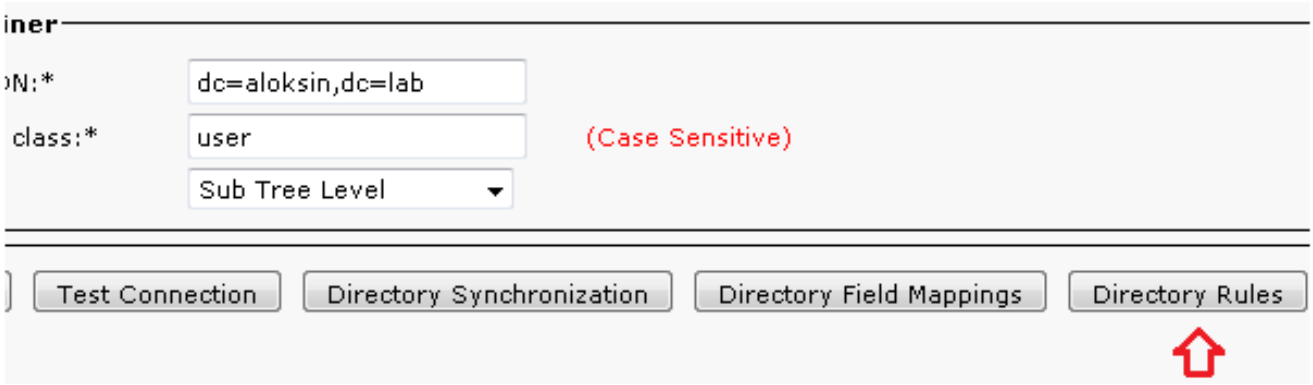
يتم إستخدام حقل *فئة الكائن* بواسطة AD لتحديد نطاق البحث المطلوب. بشكل افتراضي، يتم تعيينها إلى *جهة اتصال*، مما يعني أن AD يبحث عن *جهات اتصال* (ليس مستخدمين) في قاعدة البحث المطلوبة. لاستيراد *مستخدمين* في CUAC، قم بتغيير إعداد فئة الكائن إلى **المستخدم**:




6. احفظ الإعدادات، وانقر فوق **تعيينات حقل الدليل**، وقم بتكوين كافة السمات التي تريد إستيرادها لأي مستخدم. هنا التكوين الذي يتم إستخدامه في هذا المثال:

| Source Fields | Destination Fields | Defaul |
|---|---|---|
| telephoneNumber | Extension | |
| mail | Email | |
| givenName | First Name | |
| sn | Last Name | |

7. انتقل إلى صفحة مصدر الدليل وانقر فوق **قواعد الدليل**:

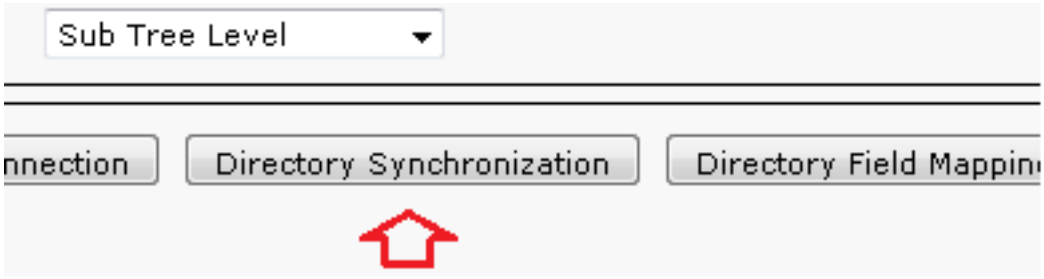



8. انقر فوق **إضافة جديد** وإنشاء قاعدة. عند إضافة قاعدة دليل، يظهر عامل تصفية القاعدة بشكل افتراضي.

| Field | Operator | Value |
|---|---|---|
| telephoneNumber | = | * |

**ملاحظة**: لا حاجة لتغيير عامل تصفية القاعدة. فهو يستورد جميع المستخدمين الذين لديهم رقم هاتف مكون.

9. لتكوين المزامنة التلقائية مع AD، انقر فوق علامة التبويب **مزامنة الدليل**.




10. اكتمل التكوين الآن. انتقل إلى **الهندسة > إدارة الخدمة** وأعد تشغيل الوظيفة الإضافية LDAP لبدء المزامنة يدويا.

# وظائف LDAP بين CUAC و AD

## ملخص عملية LDAP

فيما يلي ملخص لعملية LDAP بين CUAC و AD:

1. تم إنشاء جلسة TCP بين الخادمين (CUAC و AD).

2. يرسل CUAC طلب BIND إلى AD ويصادق عن طريق المستخدم الذي تم تكوينه في إعدادات المصادقة.

3. وبمجرد مصادقة AD للمستخدم بنجاح، يرسل إعلام نجاح BIND إلى CUACPE.

4. يرسل CUAC طلب بحث إلى AD، الذي يحتوي على معلومات نطاق البحث، مرشحات للبحث، وسمات لأي مستخدم تمت تصفيته.

5. يتم مسح AD للكائن المطلوب (المكون في إعدادات فئة الكائن) في قاعدة البحث. يقوم بتصفية الكائنات التي تطابق المعايير (عامل التصفية) المفصلة في رسالة طلب البحث.

6. يستجيب الإعلان إلى CUAC مع نتائج البحث.

هنا sniffer التقاط أن يوضح هذا steps:

| | | | |
|---|---|---|---|
| 3.208 | 10.106.98.209 | TCP | 49992 > ldap [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS= |
| 3.209 | 10.106.98.208 | TCP | ldap > 49992 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 M |
| 3.208 | 10.106.98.209 | TCP | 49992 > ldap [ACK] Seq=1 Ack=1 Win=65536 Len=0 |
| 3.208 | 10.106.98.209 | LDAP | bindRequest(3) "administrator@aloksin.lab" simple |
| 3.209 | 10.106.98.208 | LDAP | bindResponse(3) success |
| 3.208 | 10.106.98.209 | LDAP | searchRequest(4) "dc=aloksin,dc=lab" wholeSubtree |
| 3.209 | 10.106.98.208 | LDAP | searchResEntry(4) "CN=Suhail Angi,CN=Users,DC=aloksi |

## تفاصيل عملية LDAP

بمجرد اكتمال التكوين على CUAC وإعادة تشغيل مكون LDAP الإضافي، يقوم خادم CUAC بإعداد جلسة TCP باستخدام AD.

يرسل CUAC بعد ذلك طلب BIND للمصادقة مع خادم AD. إذا كانت المصادقة ناجحة، يرسل AD إستجابة نجاح الربط إلى CUAC. وبهذا، يحاول كلا الخادمين إعداد جلسة عمل على المنفذ 389 لمزامنة المستخدمين ومعلوماتهم.

فيما يلي التكوين على الخادم الذي يحدد الاسم المميز، والذي يتم إستخدامه للمصادقة في معاملة BIND:


تظهر هذه الرسائل في الربط يلتقط:

- فيما يلي مصافحة TCP، يتبعها طلب BIND:

| | | | |
|---|---|---|---|
| 98.208 | 10.106.98.209 | TCP | 50190 > ldap [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=8 |
| 98.209 | 10.106.98.208 | TCP | ldap > 50190 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MS |
| 98.208 | 10.106.98.209 | TCP | 50190 > ldap [ACK] Seq=1 Ack=1 Win=65536 Len=0 |
| 98.208 | 10.106.98.209 | LDAP | bindRequest(3) "administrator@aloksin.lab" simple |
| 98.209 | 10.106.98.208 | LDAP | bindResponse(3) success |

- فيما يلي توسيع طلب BIND:

```
Lightweight Directory Access Protocol
  LDAPMessage bindRequest(3) "administrator@aloksin.lab" simple
      messageID: 3
    protocolOp: bindRequest (0)
      bindRequest
          version: 3
          name: administrator@aloksin.lab
        authentication: simple (0)
            simple: 6331736330313233 21
    [Response To: 81]
```

- فيما يلي توسيع إستجابة BIND، الذي يشير إلى المصادقة الناجحة للمستخدم (**المسؤول** في هذا المثال):

```
Lightweight Directory Access Protocol
  LDAPMessage bindResponse(3) success
      messageID: 3
    protocolOp: bindResponse (1)
      bindResponse
          resultCode: success (0)
          matchedDN:
          errorMessage:
      [Response To: 80]
      [Time: 0.002077000 seconds]
```

عند نجاح الربط، يرسل الخادم طلب بحث إلى AD لاستيراد المستخدمين. يحتوي طلب البحث هذا على المرشح والسمات المستخدمة من قبل AD. ثم يبحث AD عن المستخدمين ضمن قاعدة البحث المحددة (كما هو مفصل في رسالة طلب البحث)، والتي تستوفي المعايير الموجودة في المرشح والتحقق من الخصائص.

هنا مثال على طلب البحث الذي تم إرساله بواسطة CUCM:

```
                                                Lightweight Directory Access Protocol
                LDAPMessage searchRequest(2) "dc=aloksin,dc=lab" wholeSubtree
                                                        messageID: 2
                                                (protocolOp: searchRequest (3
                                                        searchRequest
                                            baseObject: dc=aloksin,dc=lab
                                                    (scope: wholeSubtree (2
                                            (derefAliases: derefAlways (3
                                                        sizeLimit: 0
                                                        timeLimit: 0
                                                    typesOnly: False
                    (((Filter: (&(&(objectclass=user)(!(objectclass=Computer
                                            (((UserAccountControl:1.2.840.113556.1.4.803:=2)!)
                                                (filter: and (0
        (((and: (&(&(objectclass=user)(!(objectclass=Computer
                                            (((UserAccountControl:1.2.840.113556.1.4.803:=2)!)
                                                    and: 3 items
                                (Filter: (objectclass=user
                            (and item: equalityMatch (3
                                        equalityMatch
                        attributeDesc: objectclass
                              assertionValue: user
                            ((Filter: (!(objectclass=Computer
                                        (and item: not (2
                        (Filter: (objectclass=Computer
```

```
                (not: equalityMatch (3
                     equalityMatch
   attributeDesc: objectclass
     assertionValue: Computer
 .Filter: (!(UserAccountControl:1.2.840.113556.1.4
                                                                ((2=:803
                            (and item: not (2
Filter: (UserAccountControl:1.2.840.113556
                                                              (2=:1.4.803.
             (not: extensibleMatch (9
extensibleMatch UserAccountControl
 .matchingRule: 1.2.840.113556
                                                                   1.4.803
      type: UserAccountControl
                matchValue: 2
          dnAttributes: False
                                          attributes: 15 items
                                AttributeDescription: objectguid
                             AttributeDescription: samaccountname
                                  AttributeDescription: givenname
                                 AttributeDescription: middlename
                                        AttributeDescription: sn
                                   AttributeDescription: manager
                                AttributeDescription: department
                             AttributeDescription: telephonenumber
                                      AttributeDescription: mail
                                    AttributeDescription: title
                                 AttributeDescription: homephone
                                   AttributeDescription: mobile
                                    AttributeDescription: pager
                    AttributeDescription: msrtcsip-primaryuseraddress
                    AttributeDescription: msrtcsip-primaryuseraddress
                                                  [Response In: 103]
                                                    controls: 1 item
                                                         Control
          (controlType: 1.2.840.113556.1.4.319 (pagedResultsControl
                                                     criticality: True
                                                   SearchControlValue
                                                       size: 250
                                                  <cookie: <MISSING
```

عندما يستقبل AD هذا الطلب من CUCM، فإنه يبحث عن مستخدمين في **baseObject: dc=aloksin،dc=lab**، مما يفي بعامل التصفية. يتم تجاهل أي مستخدم لا يفي بالمتطلبات التفصيلية بواسطة عامل التصفية. يستجيب الإعلان إلى CUCM مع جميع المستخدمين الذين تمت تصفيتها ويرسل قيم السمات المطلوبة.

**ملاحظة**: لا يمكن إستيراد الكائنات. يتم إستيراد *المستخدمين* فقط. وذلك لأن عامل التصفية الذي يتم إرساله في رسالة طلب البحث يتضمن **objectClass=user**. وبالتالي، يبحث الإعلان فقط عن المستخدمين وليس جهات الاتصال. يحتوي CUCM على كل هذه التعيينات وعامل تصفية بشكل افتراضي.

لم يتم تكوين CUAC بشكل افتراضي، لا توجد تفاصيل تعيين تم تكوينها لاستيراد سمات للمستخدمين، لذلك يجب إدخال هذه التفاصيل يدويا. لإنشاء هذه التعيينات، انتقل إلى **تكوين النظام > إدارة مصدر الدليل > خدمة Active Directory > تعيين حقل الدليل**.

يسمح للمسؤولين بتعيين الحقول حسب متطلباتهم الخاصة. فيما يلي مثال:

**Directory Source**

Microsoft Active Directory

**Field Mappings**

| | | Source Fields | Destination Fields | Default Value |
|---|---|---|---|---|
| ☐ | Select | telephoneNumber | Extension | |
| ☐ | Select | mail | Email | |
| ☐ | Select | givenName | First Name | |
| ☐ | Select | sn | Last Name | |

يتم إرسال معلومات حقل المصدر إلى AD في رسالة طلب البحث. عندما يرسل الإعلان رسالة إستجابة البحث، فإن تلك القيم يتم تخزينها في الحقول المستهدفة على CUACPE.

لاحظ أن CUAC لديه بشكل افتراضي فئة الكائن معينة إلى *جهات الاتصال*. في حالة إستخدام هذا الإعداد الافتراضي، يظهر المرشح الذي يتم إرساله إلى AD كما هو موضح هنا:

```
.....  )(Filter: (&(&(objectclass=contact
```

باستخدام عامل التصفية هذا، لا يقوم AD بإرجاع أي مستخدمين إلى CUACPE، نظرا لأنه يقوم بالبحث عن *جهات الاتصال* في قاعدة البحث، وليس *المستخدمين*. لهذا السبب، يجب تغيير فئة الكائن إلى **المستخدم**:

**Container**

| | | |
|---|---|---|
| Base DN:* | dc=aloksin,dc=lab | |
| Object class:* | user | (Case Sensitive) |
| Scope: | Sub Tree Level | |

حتى هذه النقطة، هذا عملية إعداد يتلقى يكون شكلت على ال CUAC:

- تفاصيل الاتصالات
- المصادقة (مستخدم مميز للربط)
- إعدادات الحاوية
- تعيين الدليل

في هذا المثال، يتم تكوين الخاصية "فريدة" ك **sAMAccountName**. إذا قمت بإعادة تشغيل ملحق LDAP على CUAC وفحصت رسالة طلب البحث، فإنه لا يحتوي على سمات أو مرشح باستثناء **ObjectClass=user**:

```
                                    Lightweight Directory Access Protocol
LDAPMessage searchRequest(224) "dc=aloksin,dc=lab" wholeSubtree
                                                  messageID: 224
                                        (protocolOp: searchRequest (3
                                                    searchRequest
                                    baseObject: dc=aloksin,dc=lab
                                          (scope: wholeSubtree (2
                                (derefAliases: neverDerefAliases (0
                                                  sizeLimit: 1
                                                  timeLimit: 0
                                                typesOnly: True
                                          (Filter: (ObjectClass=user
                                      (filter: equalityMatch (3
                                              equalityMatch
                              attributeDesc: ObjectClass
                                    assertionValue: user
                                                attributes: 0 items
                                                    [Response In: 43]
```

لاحظ أن قاعدة الدليل مفقودة هنا. لمزامنة جهات الاتصال مع AD، يجب إنشاء قاعدة. بشكل افتراضي، لم يتم تكوين قاعدة الدليل. بمجرد إنشاء أحد المرشحات، يكون عامل التصفية موجودا بالفعل. لا حاجة لتغيير عامل التصفية، حيث يجب إستيراد كافة المستخدمين الذين لديهم رقم هاتف.

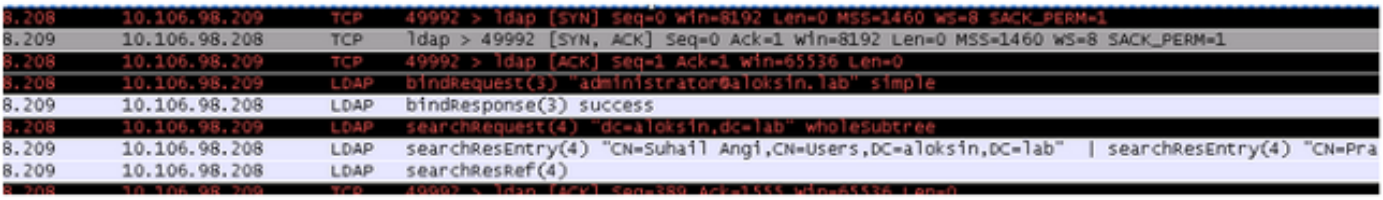
| Field | Operator | Val |
|---|---|---|
| telephoneNumber | = | * |

قم بإعادة تشغيل الوظيفة الإضافية LDAP من أجل بدء مزامنة مع AD واستيراد المستخدمين. هنا طلب البحث من CUAC:

```
                                                Lightweight Directory Access Protocol
                                    LDAPMessage searchRequest(4) "dc=aloksin,dc=lab" wholeSubtree
                                                                        messageID: 4
                                                    (protocolOp: searchRequest (3
                                                                searchRequest
                                                        baseObject: dc=aloksin,dc=lab
                                                                (scope: wholeSubtree (2
                                                (derefAliases: neverDerefAliases (0
                                                                    sizeLimit: 0
                                                                timeLimit: 15
                                                            typesOnly: False
                                        ((*=Filter: (&(&(objectclass=user)(telephoneNumber
                                                        (((UserAccountControl:1.2.840.113556.1.4.803:=2)!)
                                                                    (filter: and (0
                                    ((*=and: (&(&(objectclass=user)(telephoneNumber
                                                        (((UserAccountControl:1.2.840.113556.1.4.803:=2)!)
                                                                and: 3 items
                                                (Filter: (objectclass=user
                                            (and item: equalityMatch (3
                                                    equalityMatch
                                        attributeDesc: objectclass
                                            assertionValue: user
                                                (*=Filter: (telephoneNumber
                                                    (and item: present (7
                                                present: telephoneNumber
                                .Filter: (!(UserAccountControl:1.2.840.113556
                                                                                                ((2=:1.4.803
                                                        (and item: not (2
                                .Filter: (UserAccountControl:1.2.840.113556
                                                                                                (2=:1.4.803
                                            (not: extensibleMatch (9
                                 extensibleMatch UserAccountControl
                                .matchingRule: 1.2.840.113556.1
                                                                                                    4.803
                                    type: UserAccountControl
                                            matchValue: 2
                                        dnAttributes: False
                                                                    attributes: 10 items
                                                AttributeDescription: TELEPHONENUMBER
                                                            AttributeDescription: MAIL
                                                        AttributeDescription: GIVENNAME
                                                                AttributeDescription: SN
                                                    AttributeDescription: sAMAccountName
                                                        AttributeDescription: ObjectClass
                                                        AttributeDescription: whenCreated
                                                        AttributeDescription: whenChanged
                                                        AttributeDescription: uSNCreated
                                                        AttributeDescription: uSNChanged
                                                                    [Response In: 11405]
                                                                        controls: 1 item
```

```
                                                    Control
            (controlType: 1.2.840.113556.1.4.319 (pagedResultsControl
                                                  SearchControlValue
                                                      size: 500
                                                  <cookie: <MISSING
```

إذا وجد AD مستخدمين يتطابقون مع المعايير المفصلة في رسالة طلب البحث، يرسل بعد ذلك رسالة *SearchResEntry* التي تحتوي على معلومات المستخدم.




فيما يلي رسالة SearchResEntry:

```
                                                Lightweight Directory Access Protocol
[LDAPMessage searchResEntry(4) "CN=Suhail Angi,CN=Users,DC=aloksin,DC=lab" [4 results
                                                                messageID: 4
                                                (protocolOp: searchResEntry (4
                                                            searchResEntry
                                objectName: CN=Suhail Angi,CN=Users,DC=aloksin,DC=lab
                                                        attributes: 9 items
                                    PartialAttributeList item objectClass
                                                    type: objectClass
                                                        vals: 4 items
                                                              top
                                                           person
                                                organizationalPerson
                                                             user
                                    PartialAttributeList item sn
                                                    type: sn
                                                        vals: 1 item
                                                           Angi
                                PartialAttributeList item telephoneNumber
                                                type: telephoneNumber
                                                        vals: 1 item
                                                           1002
                                  PartialAttributeList item givenName
                                                    type: givenName
                                                        vals: 1 item
                                                          Suhail
                                PartialAttributeList item whenCreated
                                                type: whenCreated
                                                        vals: 1 item
                                                20131222000850.0Z
                                PartialAttributeList item whenChanged
                                                type: whenChanged
                                                        vals: 1 item
                                                20131222023413.0Z
                                 PartialAttributeList item uSNCreated
                                                type: uSNCreated
                                                        vals: 1 item
                                                           12802
                                 PartialAttributeList item uSNChanged
                                                type: uSNChanged
                                                        vals: 1 item
                                                           12843
                               PartialAttributeList item sAMAccountName
                                                type: sAMAccountName
```

```
                                                vals: 1 item
                                                   sangi
                                                        [Response To: 11404]
                                                  [Time: 0.001565000 seconds]
                                               Lightweight Directory Access Protocol
[LDAPMessage searchResEntry(4) "CN=Pragathi NS,CN=Users,DC=aloksin,DC=lab" [5 results
                                                                  messageID: 4
                                                (protocolOp: searchResEntry (4
                                                             searchResEntry
                          objectName: CN=Pragathi NS,CN=Users,DC=aloksin,DC=lab
                                                    attributes: 9 items
                               PartialAttributeList item objectClass
                                              type: objectClass
                                                  vals: 4 items
                                                        top
                                                     person
                                          organizationalPerson
                                                       user
                                          PartialAttributeList item sn
                                                       type: sn
                                                    vals: 1 item
                                                          NS
                                  PartialAttributeList item telephoneNumber
                                                type: telephoneNumber
                                                    vals: 1 item
                                                       1000
                                                    .......
                                  ..........{message truncated}....
                                                    .....
```

**ملاحظة**: لا يوجد بريد في الاستجابة، على الرغم من طلب هذه السمة. وذلك لأنه لم يتم تكوين معرف البريد للمستخدمين على AD.

بمجرد إستلام هذه القيم بواسطة CUAC، فإنها تخزنها في جدول لغة الاستعلام المنظمة (SQL). يمكنك بعد ذلك تسجيل الدخول إلى وحدة التحكم، وتحضر وحدة التحكم قائمة المستخدمين من جدول SQL هذا على خادم CUACPE.

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).