Integrating with Active Directory

arek@arekdreyer.com

MacSysAdmin 2010

Remember

- Identification
- Authentication
- Authorization
- (and client management)

75 minutes

- Why Integrate
- 3 Challenges
- Terminology Agreement
- 4 Integration Strategies
- 15 Issues unique to AD integration

Why Integrate with AD

- Access AD's centralized store
  - LDAP
  - Kerberos
- AD is already there
- AD is ... pretty good

Challenges

- Managed Preferences for Apple objects
- Accessing DFS Shares
- Cleartext

Challenge 1

- No apple objects and attributes

Challenge 2

- DFS

Challenge 3

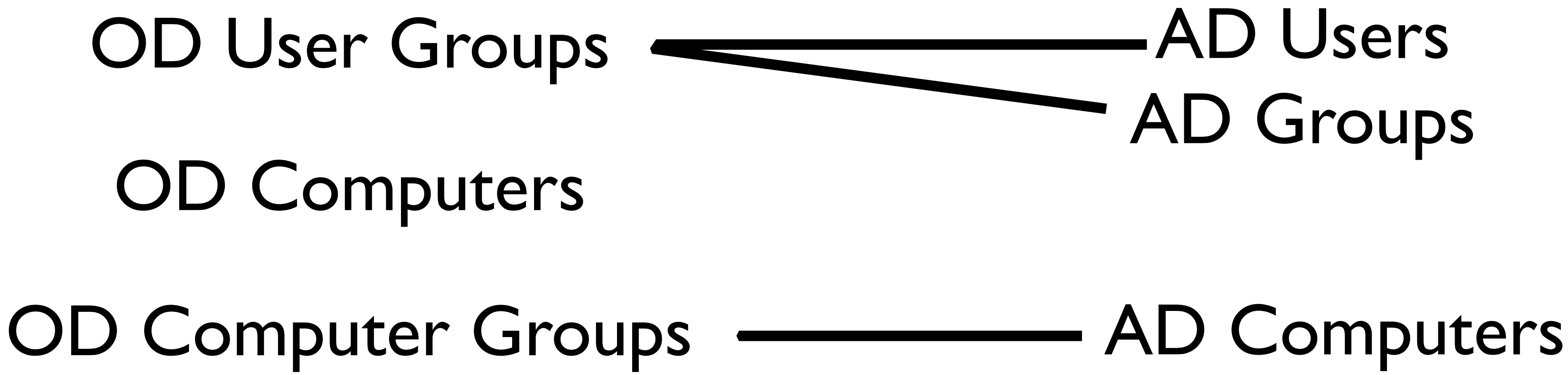
- Pass cleartext authentication to AD
  - Mac OS X Server services

Terminology Sidebar

- Dual Directory/____ Triangle
- Plugin/Connector
- Directory/Folder
- Augment Records/Cylinder of Destiny

What kind of Triangle?

- Magic Triangle
- Golden Triangle
- Dual Directory



OD User Groups

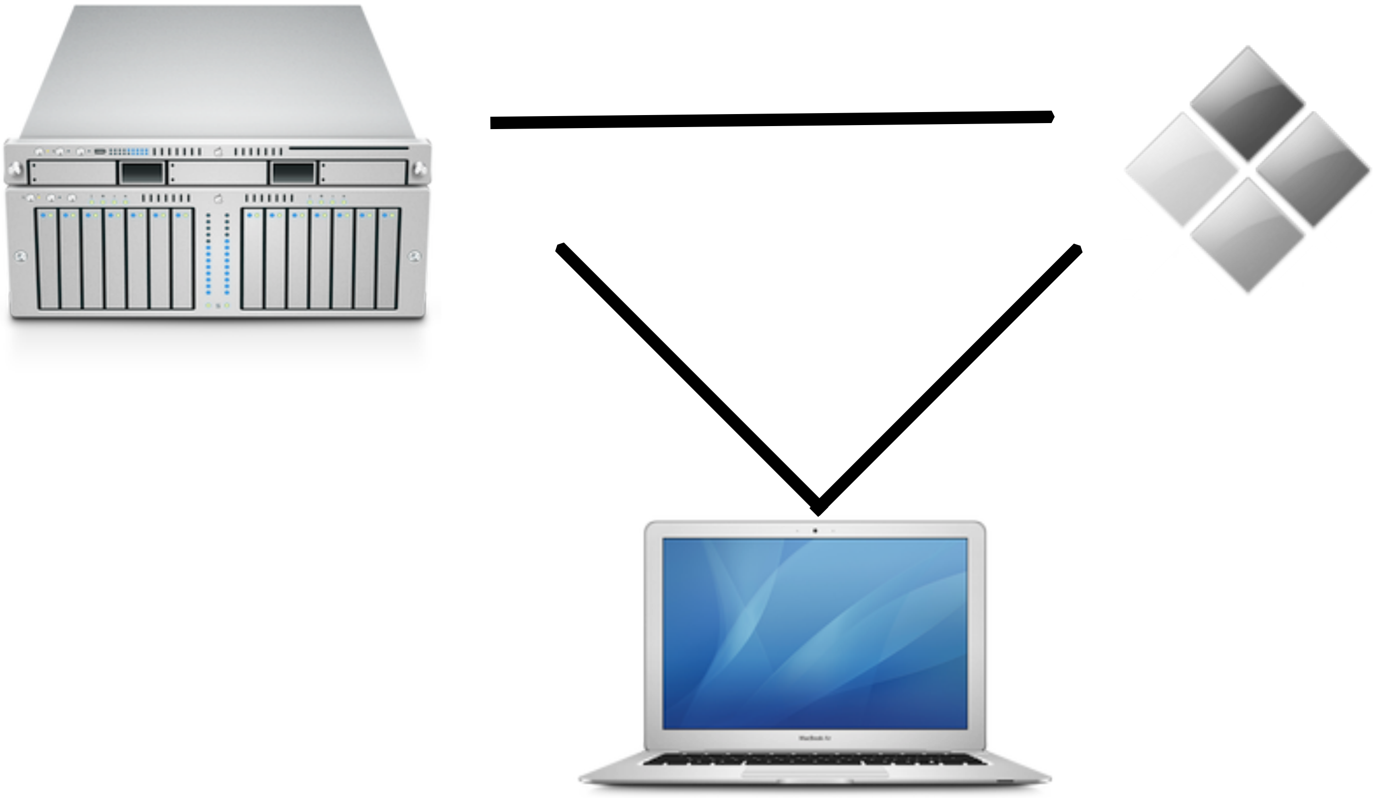
AD Users

AD Groups

OD Computers

OD Computer Groups

AD Computers

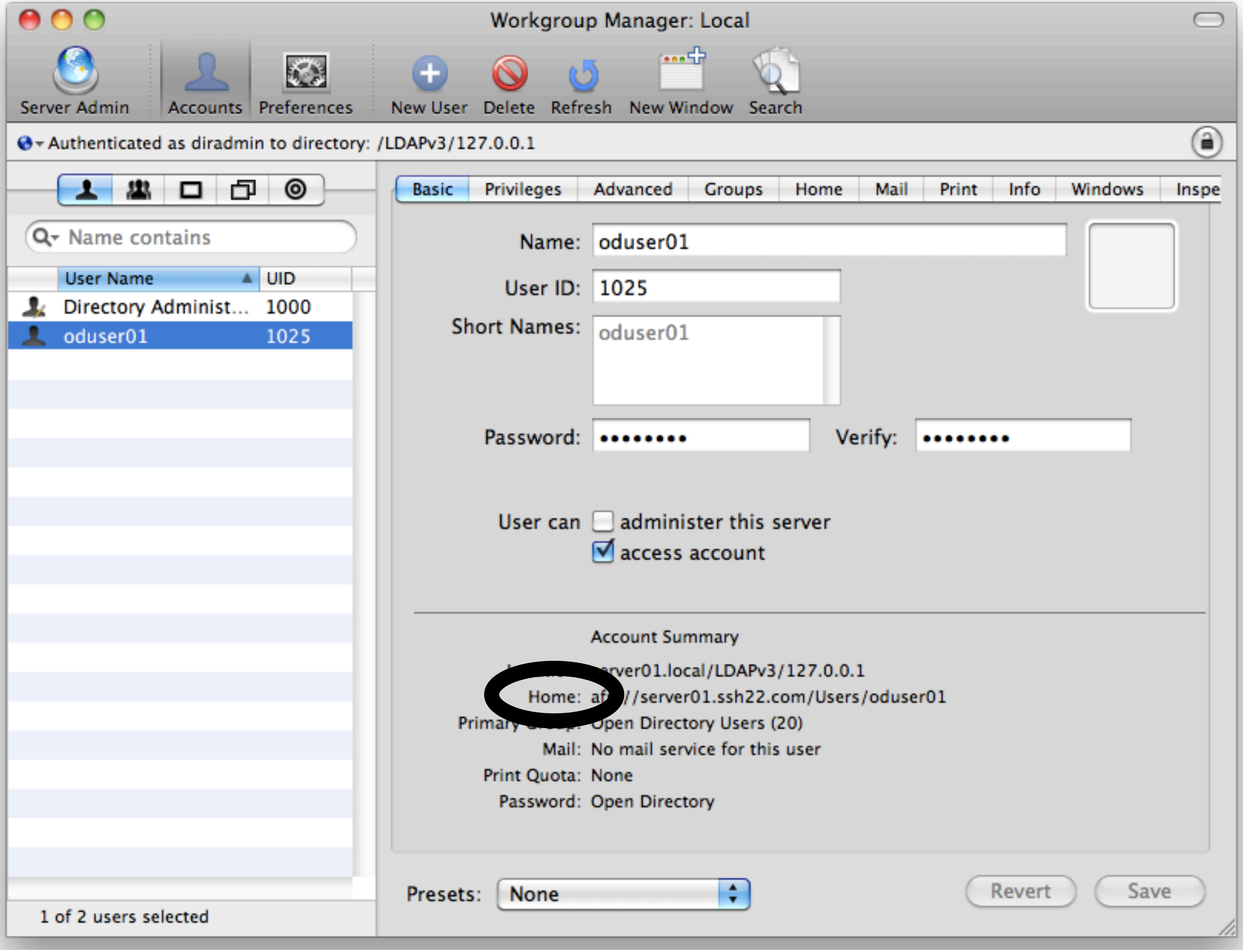


Plugin or Connector?

- Depends on who you ask

PHD?!

- Portable Home Directory
- But it is a Folder, not a Directory!
- Oh well



Authenticated as diradmin to directory: /LDAPv3/127.0.0.1

User Name	UID
Directory Administ...	1000
oduser01	1025

1 of 2 users selected

Name: oduser01

User ID: 1025

Short Names: oduser01

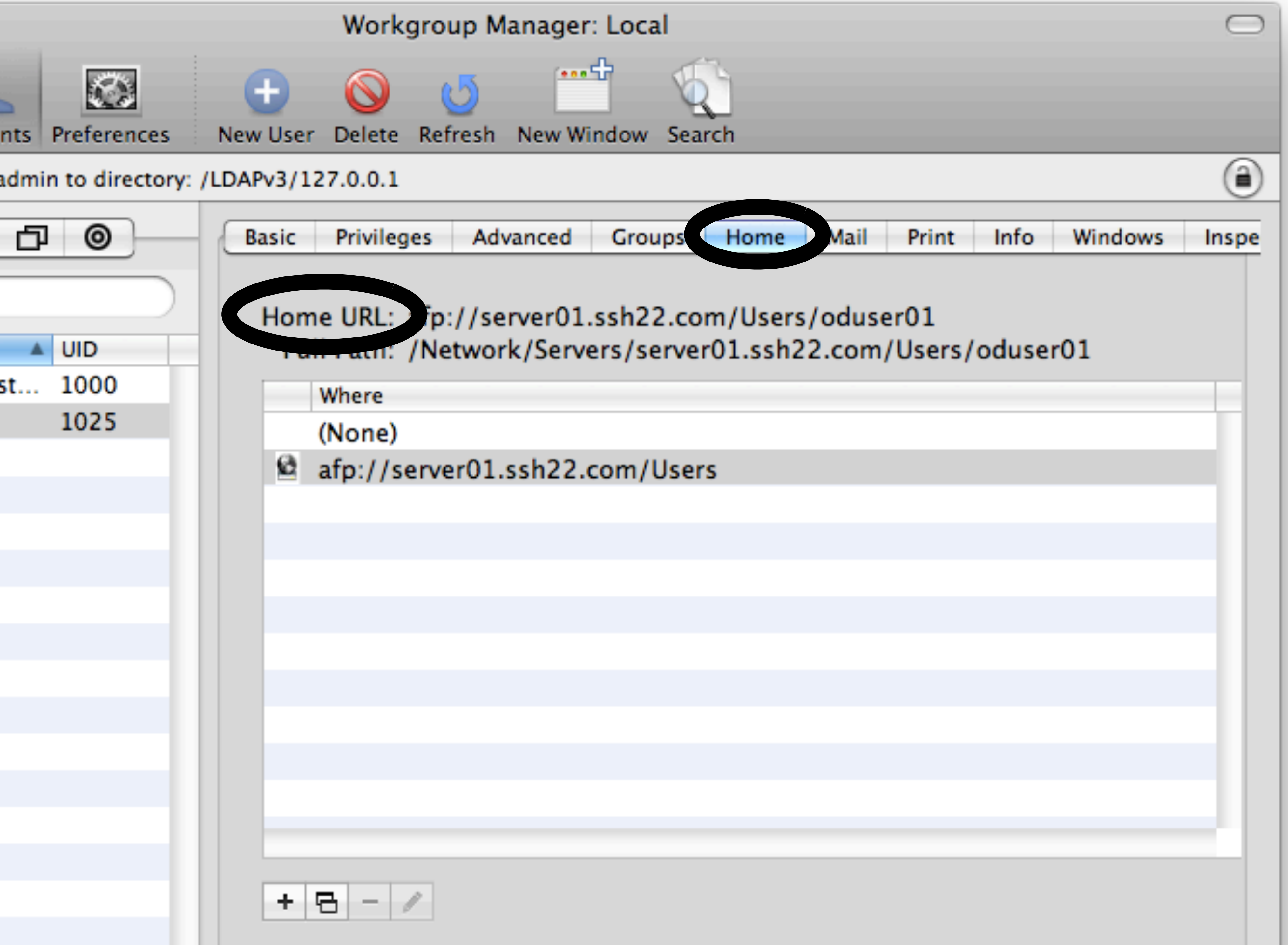
Password: •••••••• Verify: ••••••••

User can ☐ administer this server
☑ access account

Account Summary

rver01.local/LDAPv3/127.0.0.1
Home: afp://server01.ssh22.com/Users/oduser01
Primary Group: Open Directory Users (20)
Mail: No mail service for this user
Print Quota: None
Password: Open Directory

Presets: None

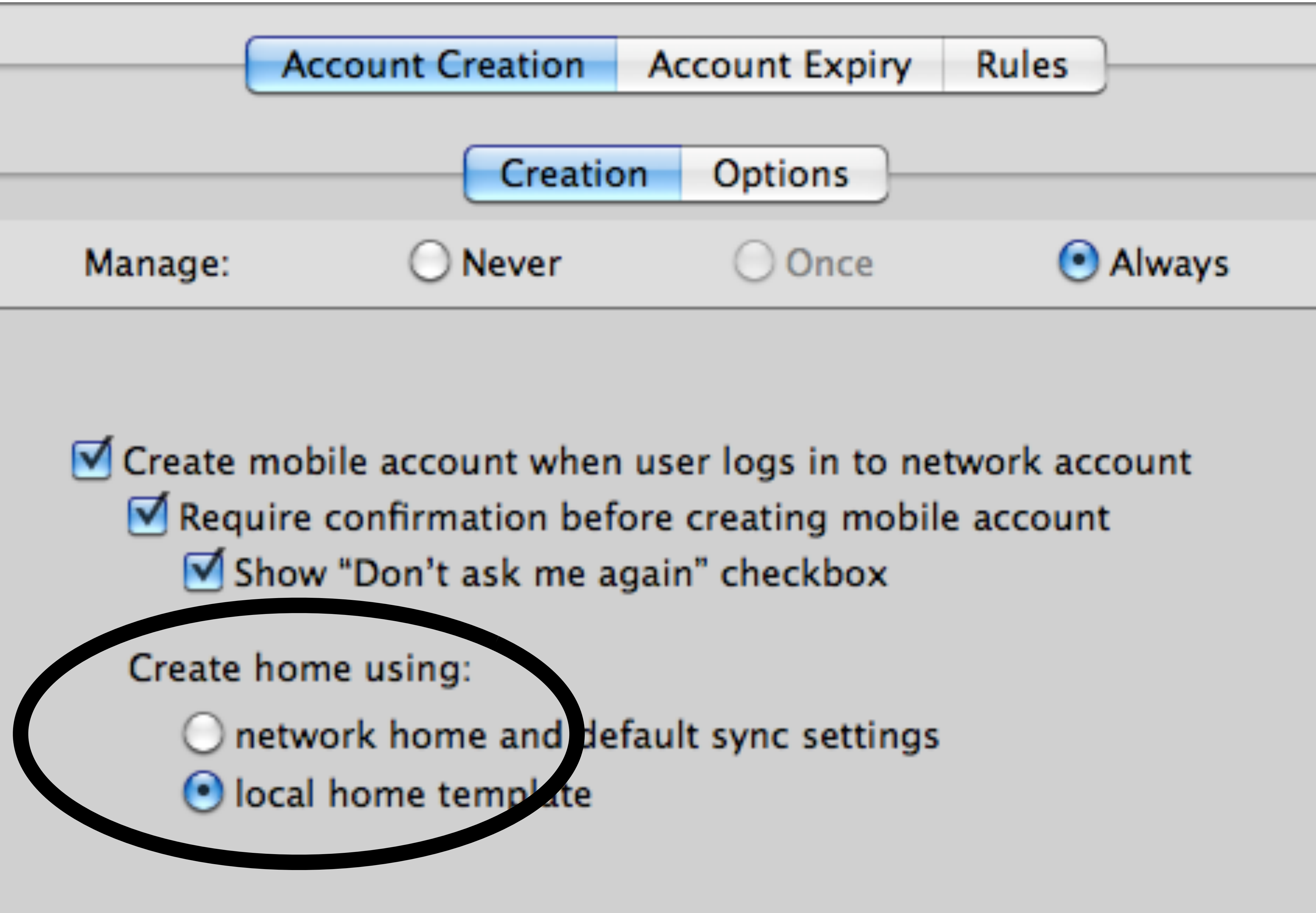


UID
1000
1025

Home URL: fp://server01.ssh22.com/Users/oduser01

/Network/Servers/server01.ssh22.com/Users/oduser01

Where
(None)
afp://server01.ssh22.com/Users



Manage: ○ Never ○ Once ● Always

☑ Create mobile account when user logs in to network account

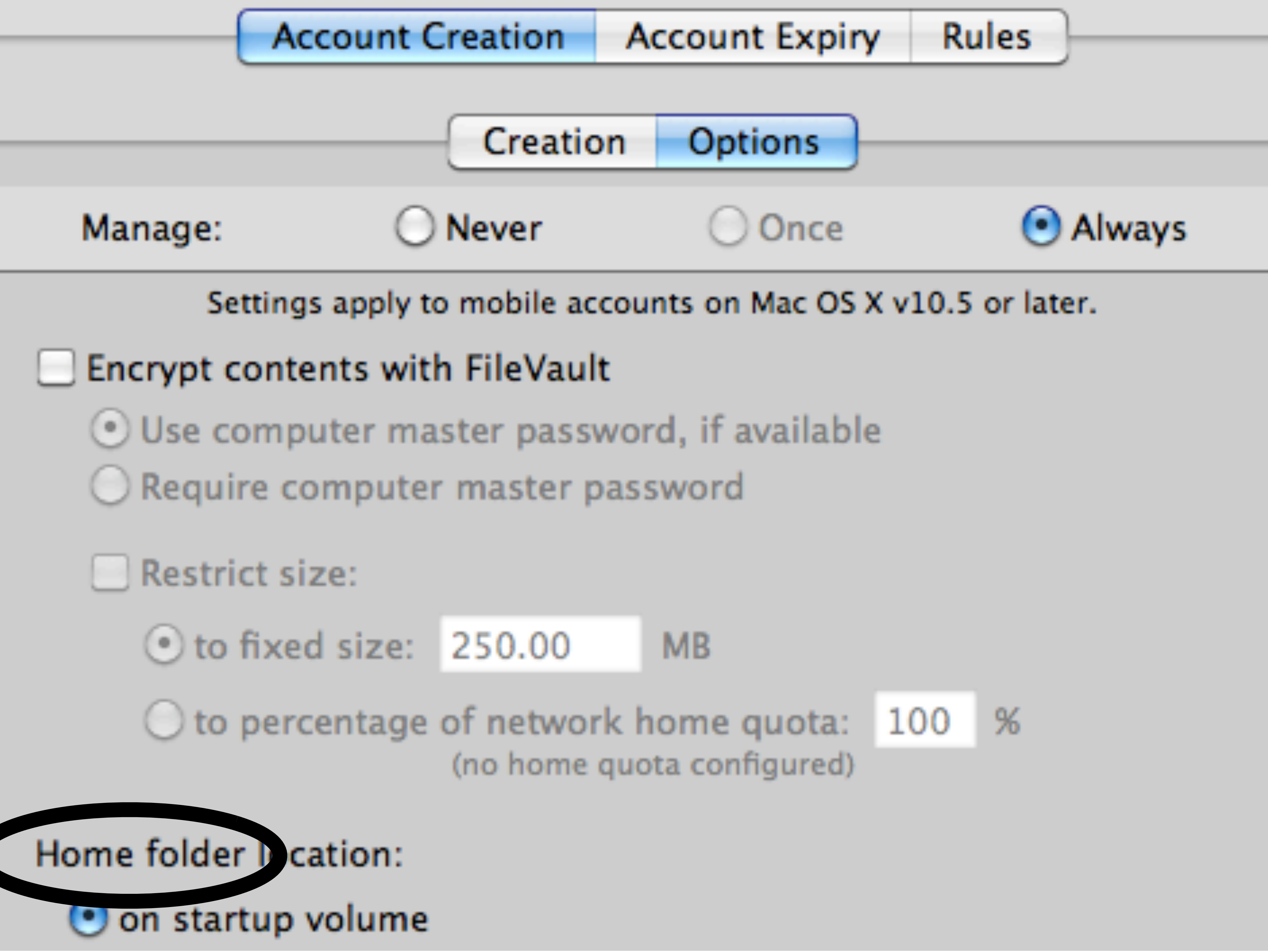
☑ Require confirmation before creating mobile account

☑ Show "Don't ask me again" checkbox

Create home using:

○ network home and default sync settings

● local home template



Manage: ○ Never ○ Once ● Always

Settings apply to mobile accounts on Mac OS X v10.5 or later.

□ Encrypt contents with FileVault

● Use computer master password, if available

○ Require computer master password

□ Restrict size:

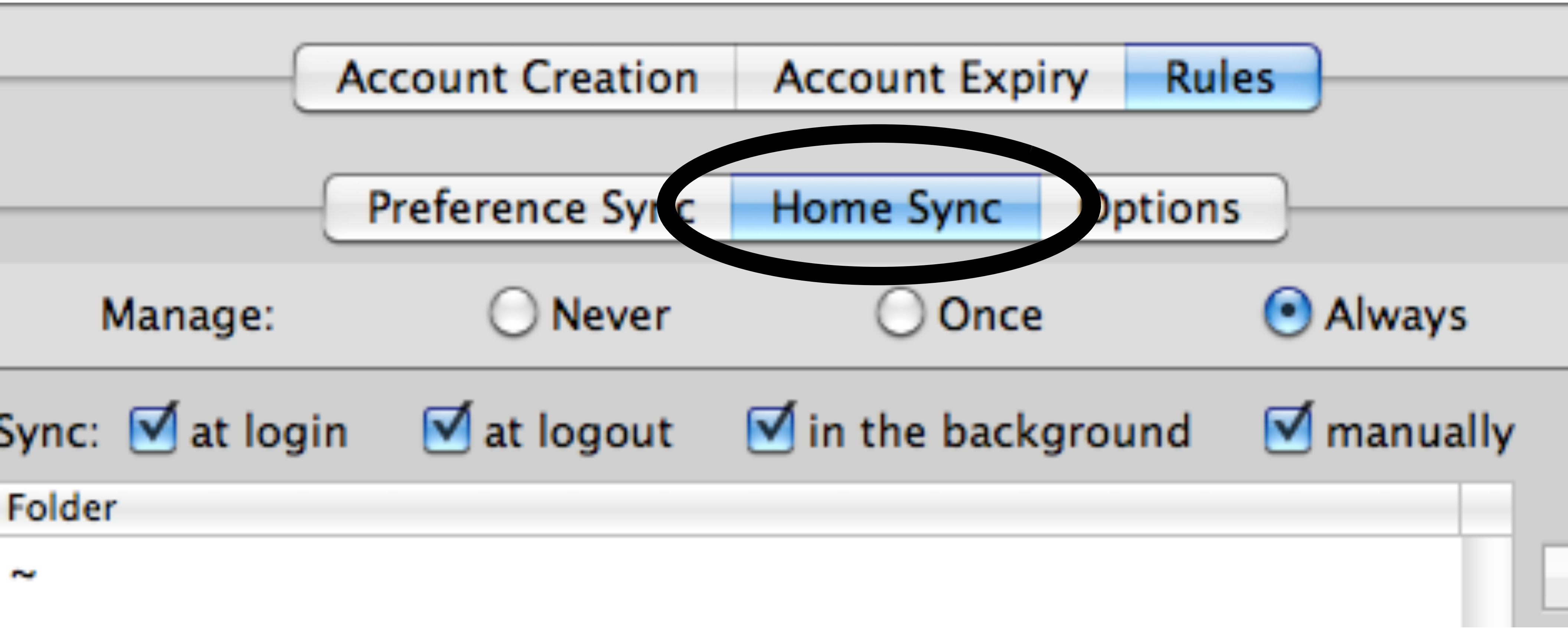
● to fixed size: 250.00 MB

○ to percentage of network home quota: 100 %

(no home quota configured)

Home folder location:

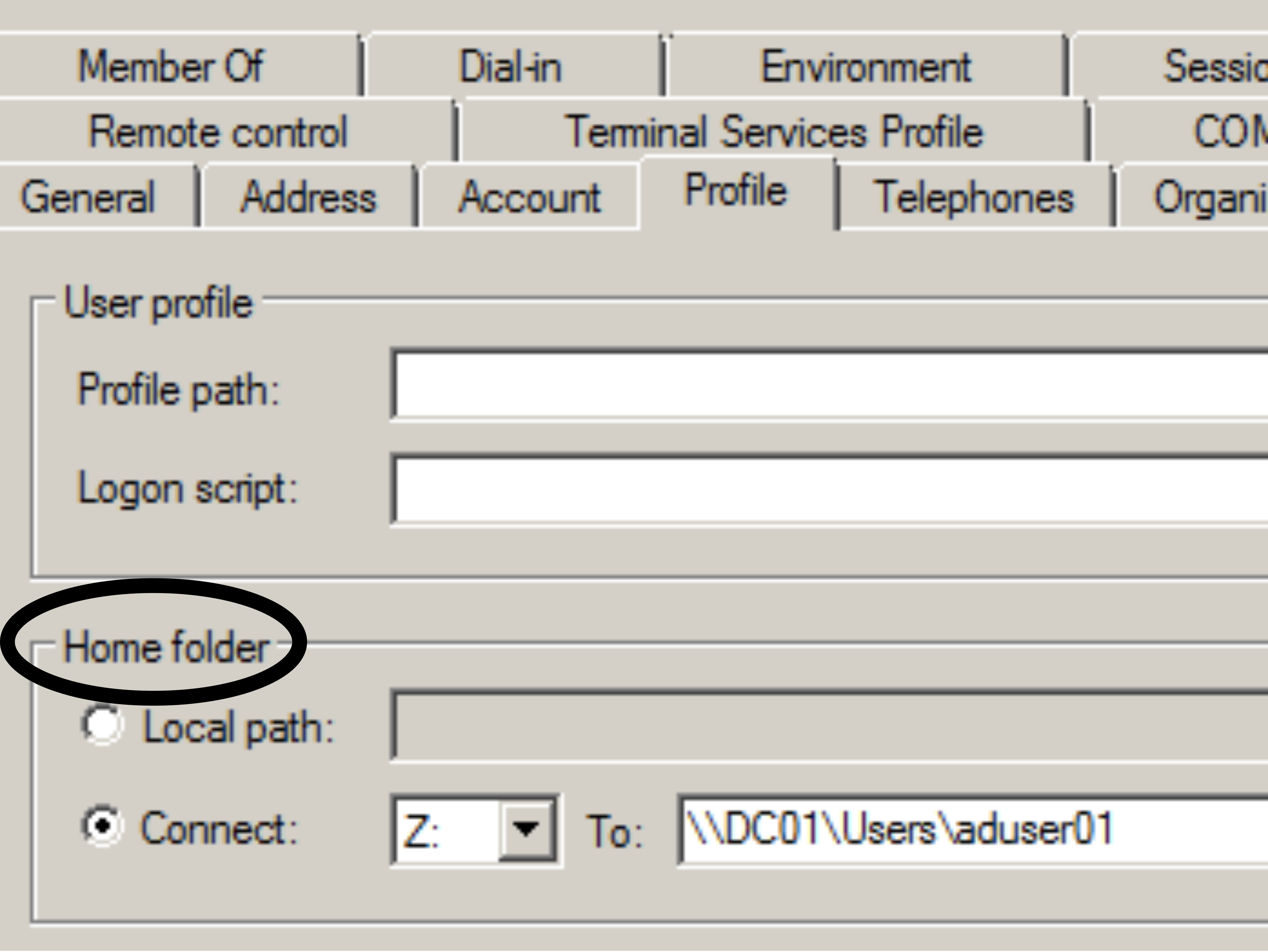
● on startup volume



Manage: ○ Never ○ Once ● Always

Sync: ☑ at login ☑ at logout ☑ in the background ☑ manually

Folder
~



User profile

Profile path:

Logon script:

Home folder

○ Local path:

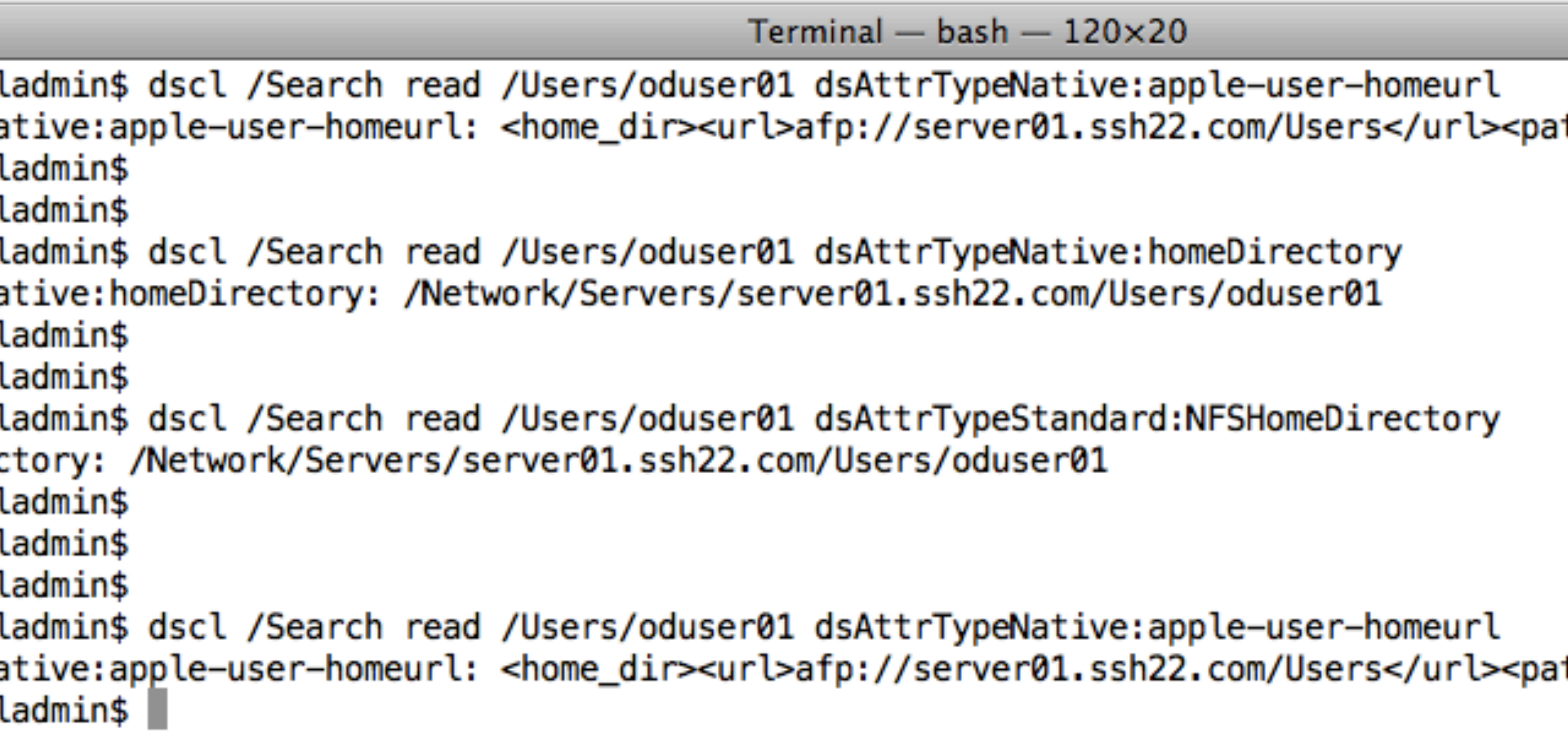
● Connect: Z: To: \\DC01\Users\aduser01

dsAttrTypeNative

- LDAP from OD
  - apple-user-homeurl
  - homeDirectory
- LDAP from AD
  - SMBHome

dsAttrTypeStandard

- dscl says:
    - homeDirectory
    - NFSHomeDirectory
    - SMBHome



```
ladmin$ dscl /Search read /Users/oduser01 dsAttrTypeNative:apple-user-homeurl
ative:apple-user-homeurl: <home_dir><url>afp://server01.ssh22.com/Users</url><pat
ladmin$
ladmin$
ladmin$ dscl /Search read /Users/oduser01 dsAttrTypeNative:homeDirectory
ative:homeDirectory: /Network/Servers/server01.ssh22.com/Users/oduser01
ladmin$
ladmin$
ladmin$ dscl /Search read /Users/oduser01 dsAttrTypeStandard:NFSHomeDirectory
ctory: /Network/Servers/server01.ssh22.com/Users/oduser01
ladmin$
ladmin$
ladmin$
ladmin$ dscl /Search read /Users/oduser01 dsAttrTypeNative:apple-user-homeurl
ative:apple-user-homeurl: <home_dir><url>afp://server01.ssh22.com/Users</url><pat
ladmin$
```

Cylinder of Destiny

- Augment Record
    - Not standard
    - Not really necessary
    - Move along

Terminology Review

- Dual Directory/_____ Triangle
- Plugin/Connector
- Directory/Folder
- Augment Records/Cylinder of Destiny

Remember: Challenges

- Managed Preferences for Apple objects
- Accessing DFS Shares
- Cleartext

4 Integration Strategies

- Bind to AD only
- Bind to AD and extend AD
- Dual Directory
- Third-party

1: Bind to AD Only

- If you have
  - Robust AD environment
  - Many locations
  - Implemented AD Sites

1: Bind to AD Only

- Advantages
  - Don't need parallel OD systems
  - Possible to auto mount SMBHome
- Disadvantage
  - Can't apply managed preferences

2: Extend Schema

- If you have Great AD infrastructure
- Manage preferences with WGM

Extending the Schema

- Well documented now
  - LDS to compare AD and OD schema
  - Edit difference LDIF
  - Import LDIF into AD
  - WGM to manage preferences
  - dscl/ADSIEDit to create computer lists

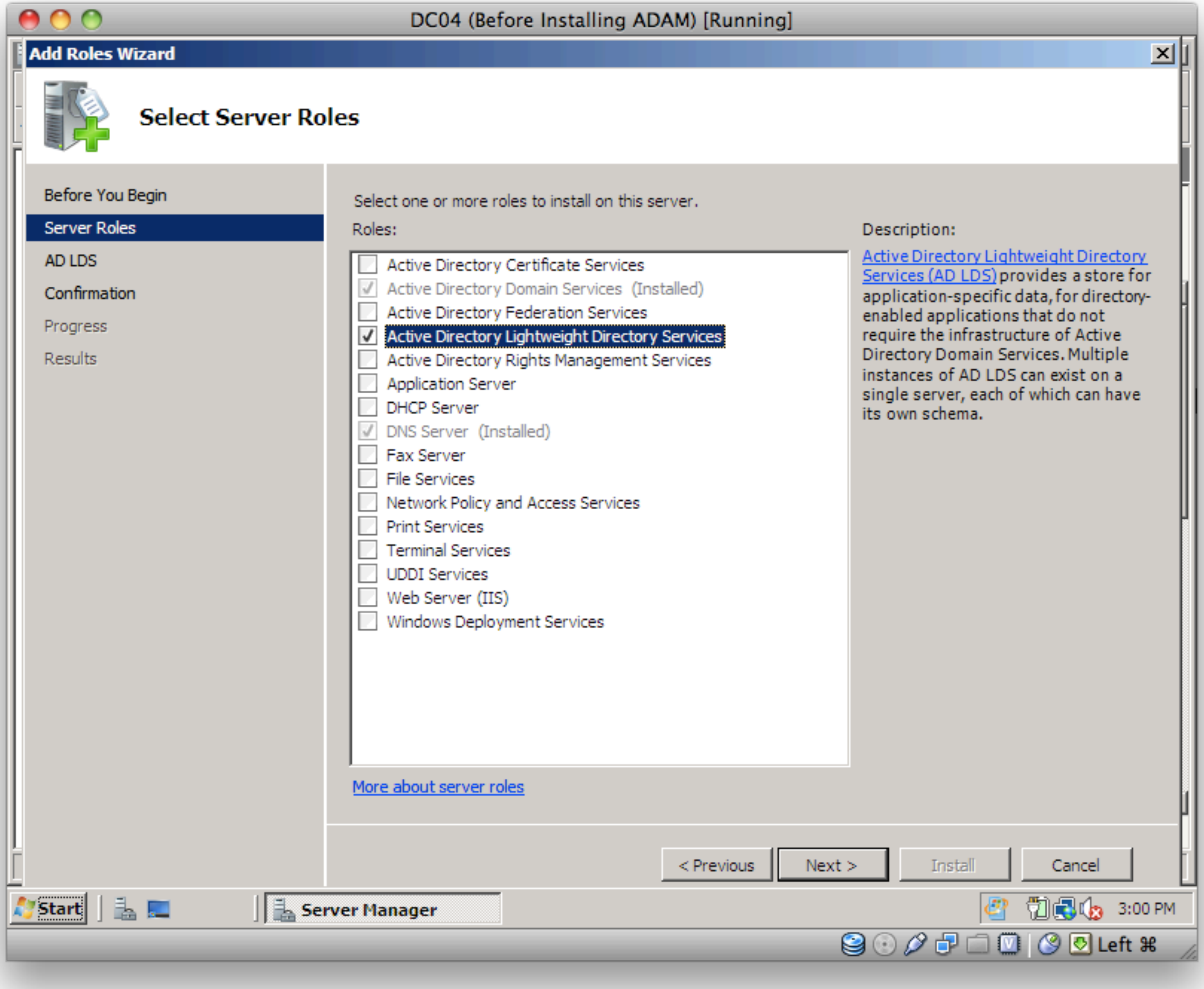
Well Documented

- Marczak/Neagle: Page 71-90
- http://images.apple.com/business/solutions\

  /it/docs/Modifying_the_Active_Directory_Schema.pdf
- Movie gone

22 Simple Steps

- In 3 minutes



DC04 (Before Installing ADAM) [Running]

Add Roles Wizard

Select Server Roles

- Before You Begin
- Server Roles
- AD LDS
- Confirmation
- Progress
- Results

Select one or more roles to install on this server.

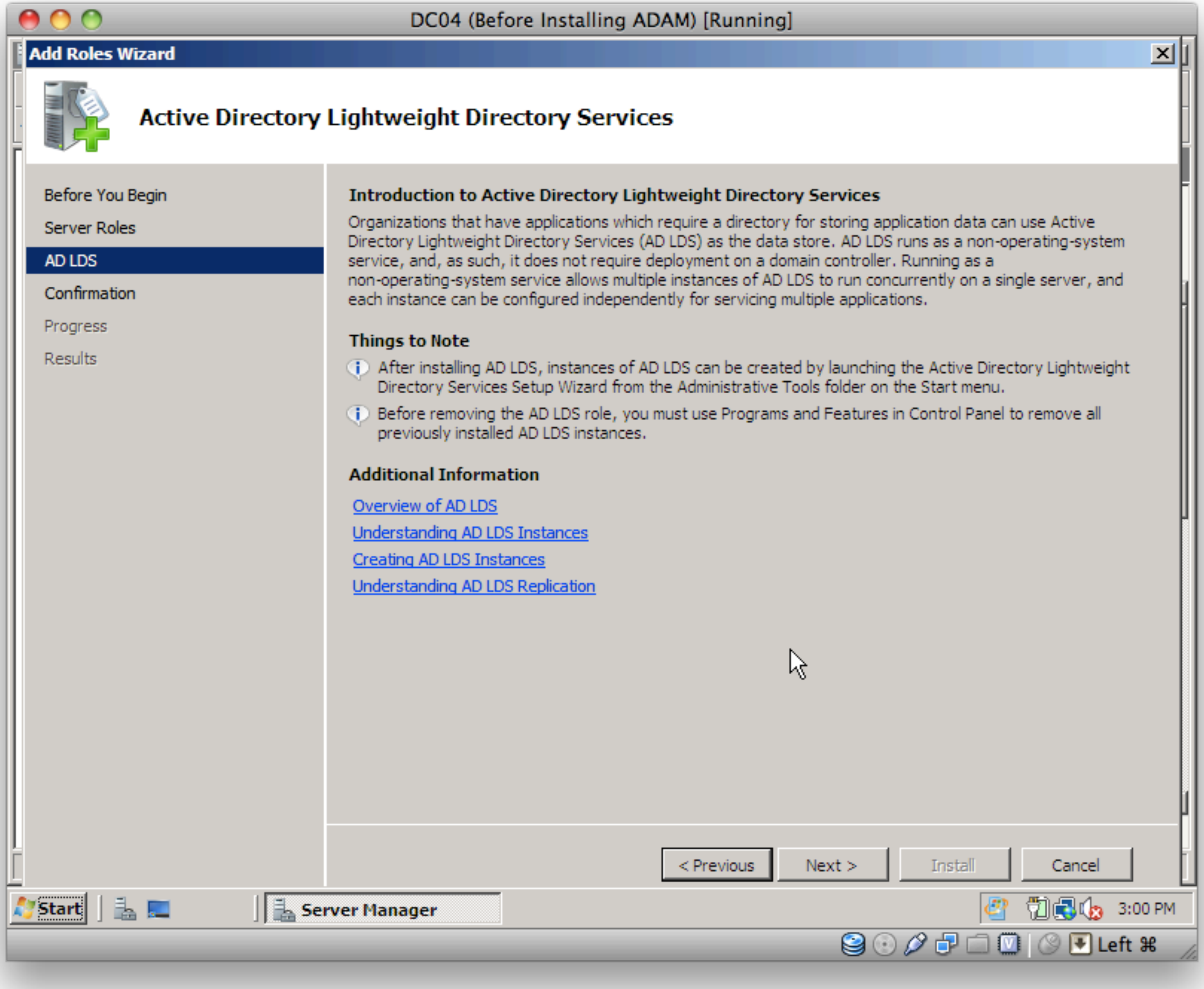
Roles:

- ☐ Active Directory Certificate Services
- ☑ Active Directory Domain Services (Installed)
- ☐ Active Directory Federation Services
- ☑ Active Directory Lightweight Directory Services
- ☐ Active Directory Rights Management Services
- ☐ Application Server
- ☐ DHCP Server
- ☑ DNS Server (Installed)
- ☐ Fax Server
- ☐ File Services
- ☐ Network Policy and Access Services
- ☐ Print Services
- ☐ Terminal Services
- ☐ UDDI Services
- ☐ Web Server (IIS)
- ☐ Windows Deployment Services

Description:

Active Directory Lightweight Directory Services (AD LDS) provides a store for application-specific data, for directory-enabled applications that do not require the infrastructure of Active Directory Domain Services. Multiple instances of AD LDS can exist on a single server, each of which can have its own schema.

More about server roles



Active Directory Lightweight Directory Services

Introduction to Active Directory Lightweight Directory Services

Organizations that have applications which require a directory for storing application data can use Active Directory Lightweight Directory Services (AD LDS) as the data store. AD LDS runs as a non-operating-system service, and, as such, it does not require deployment on a domain controller. Running as a non-operating-system service allows multiple instances of AD LDS to run concurrently on a single server, and each instance can be configured independently for servicing multiple applications.

Things to Note

- After installing AD LDS, instances of AD LDS can be created by launching the Active Directory Lightweight Directory Services Setup Wizard from the Administrative Tools folder on the Start menu.
- Before removing the AD LDS role, you must use Programs and Features in Control Panel to remove all previously installed AD LDS instances.

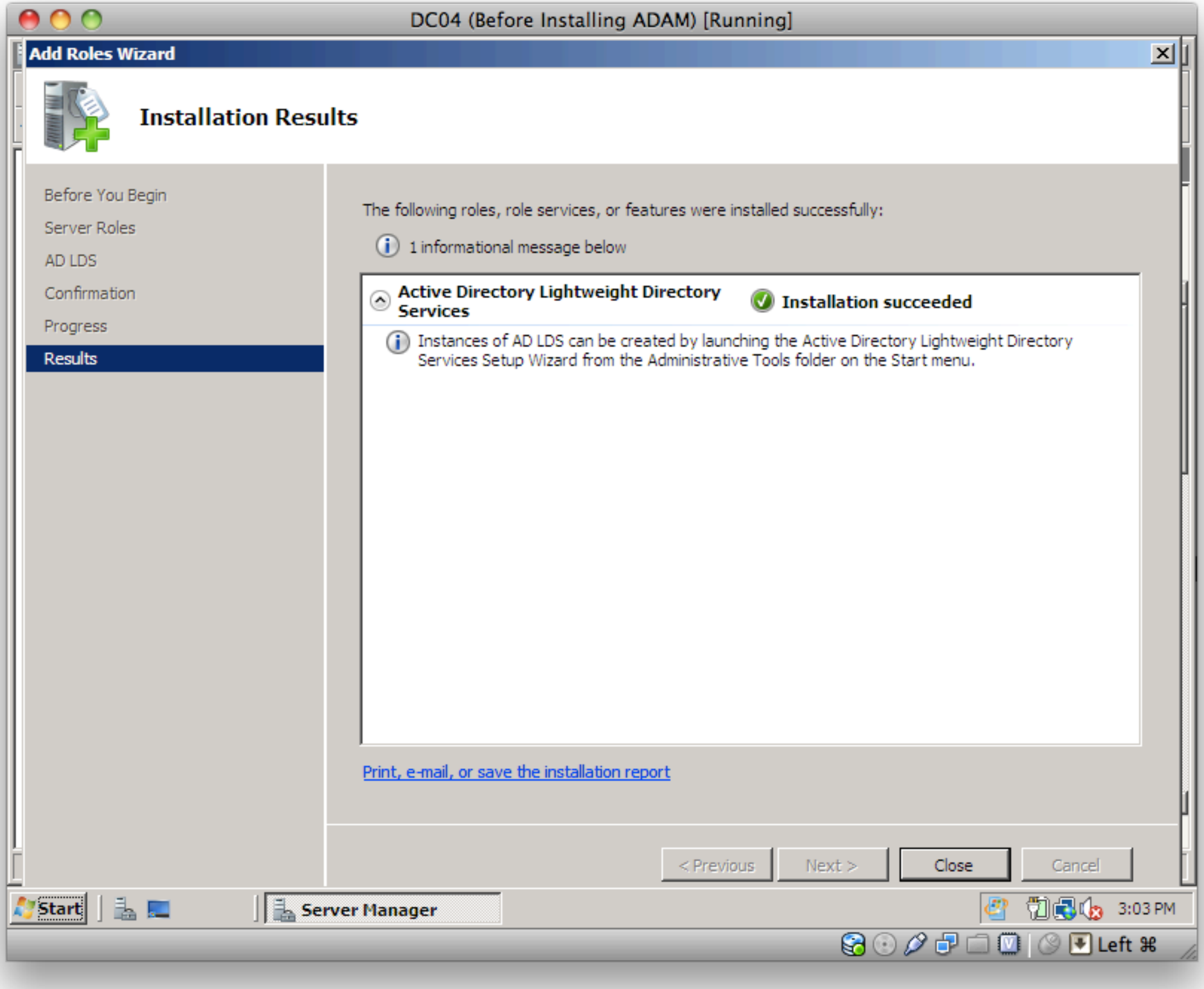
Additional Information

Overview of AD LDS

Understanding AD LDS Instances

Creating AD LDS Instances

Understanding AD LDS Replication



DC04 (Before Installing ADAM) [Running]

Add Roles Wizard

Installation Results

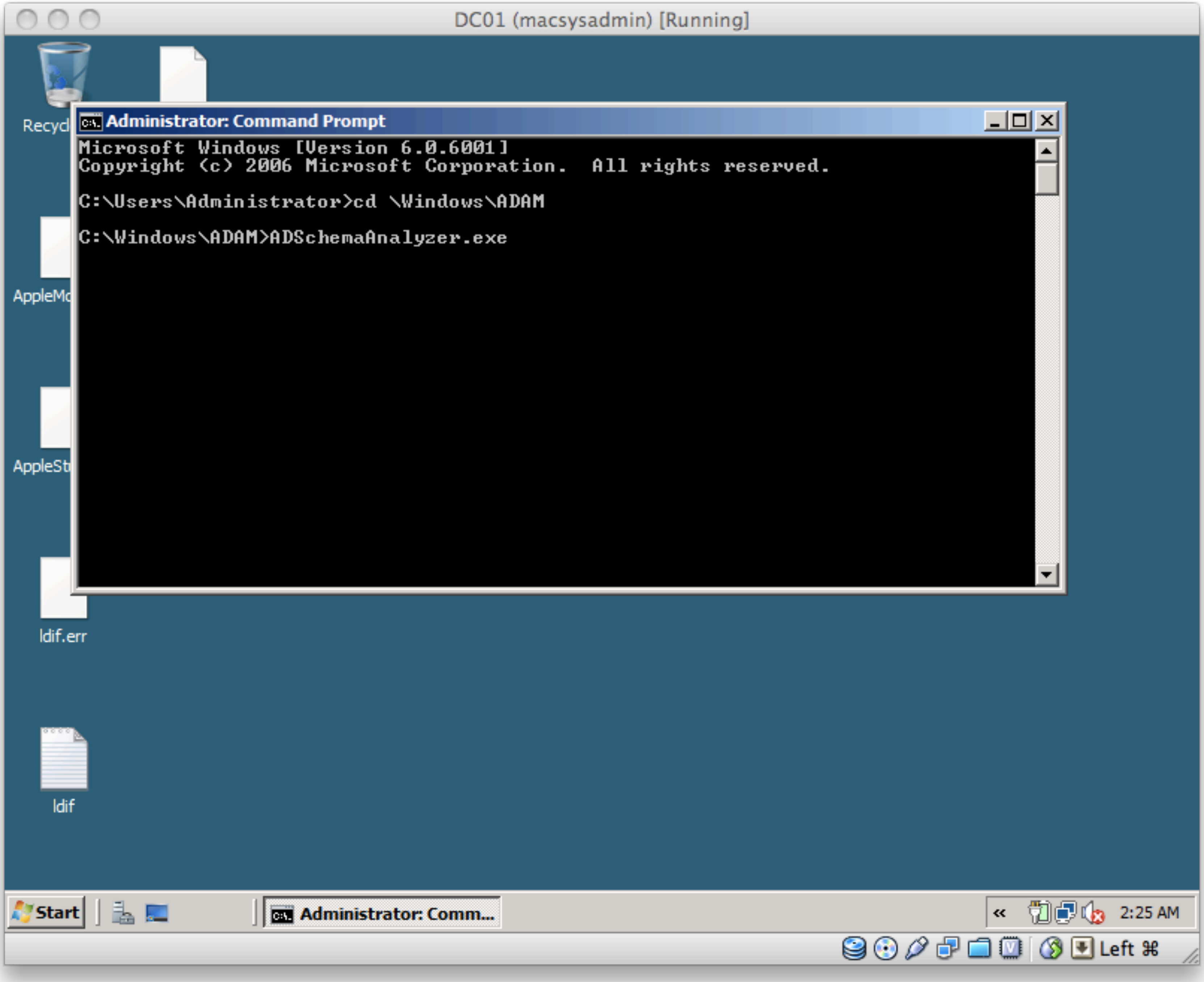
The following roles, role services, or features were installed successfully:

1 informational message below

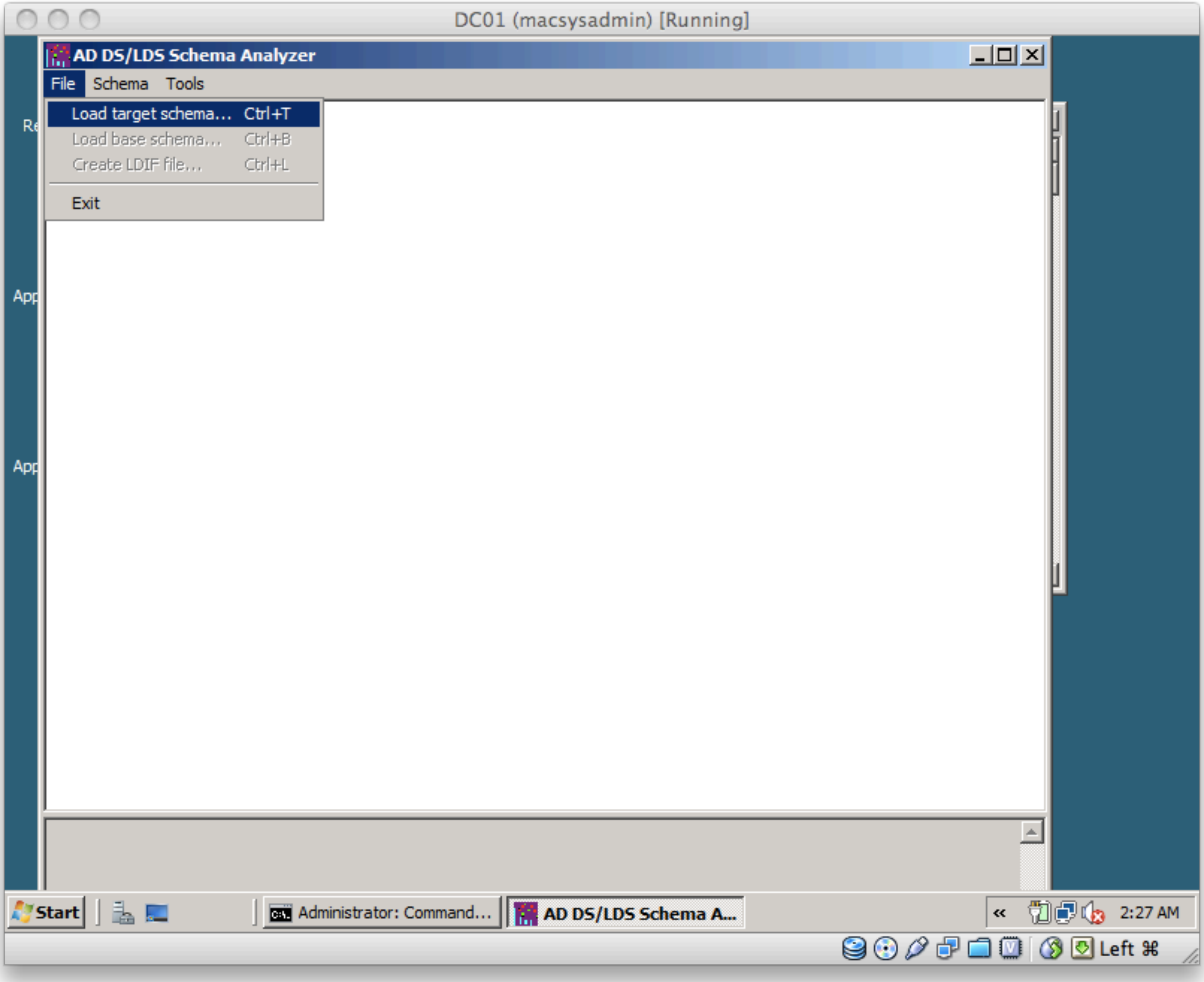
Active Directory Lightweight Directory Services ✓ Installation succeeded

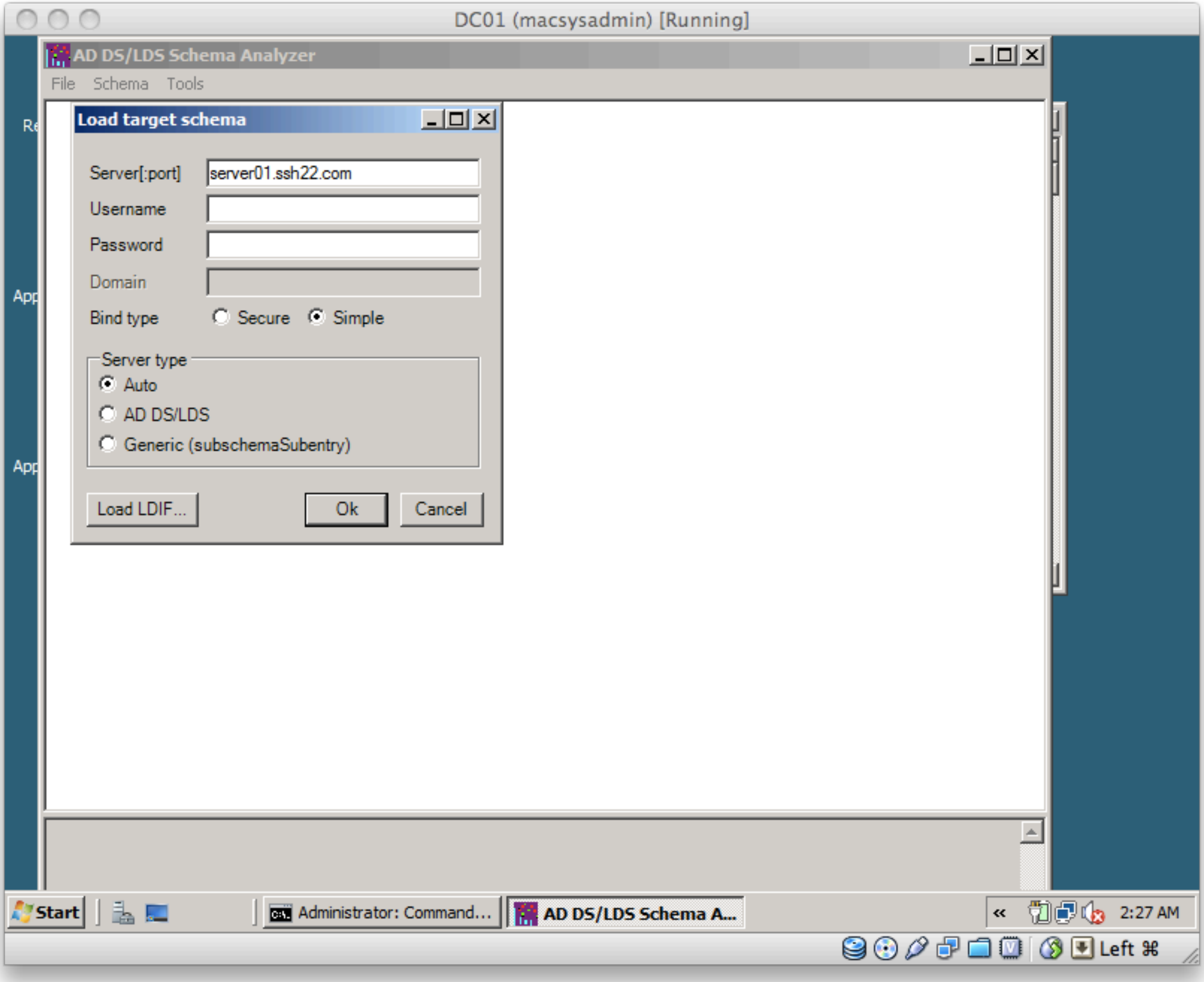
Instances of AD LDS can be created by launching the Active Directory Lightweight Directory Services Setup Wizard from the Administrative Tools folder on the Start menu.

Print, e-mail, or save the installation report



```
Microsoft Windows [Version 6.0.6001]
Copyright (c) 2006 Microsoft Corporation.  All rights reserved.

C:\Users\Administrator>cd \Windows\ADAM

C:\Windows\ADAM>ADSchemaAnalyzer.exe
```


DC01 (macsysadmin) [Running]
AD DS/LDS Schema Analyzer
File
Schema
Tools
Load target schema... Ctrl+T
Load base schema... Ctrl+B
Create LDIF file... Ctrl+L
Exit
Start
Administrator: Command...
AD DS/LDS Schema A...
2:27 AM
Left ⌘



DC01 (macsysadmin) [Running]

AD DS/LDS Schema Analyzer

Load target schema

Server[:port] server01.ssh22.com

Username

Password

Domain

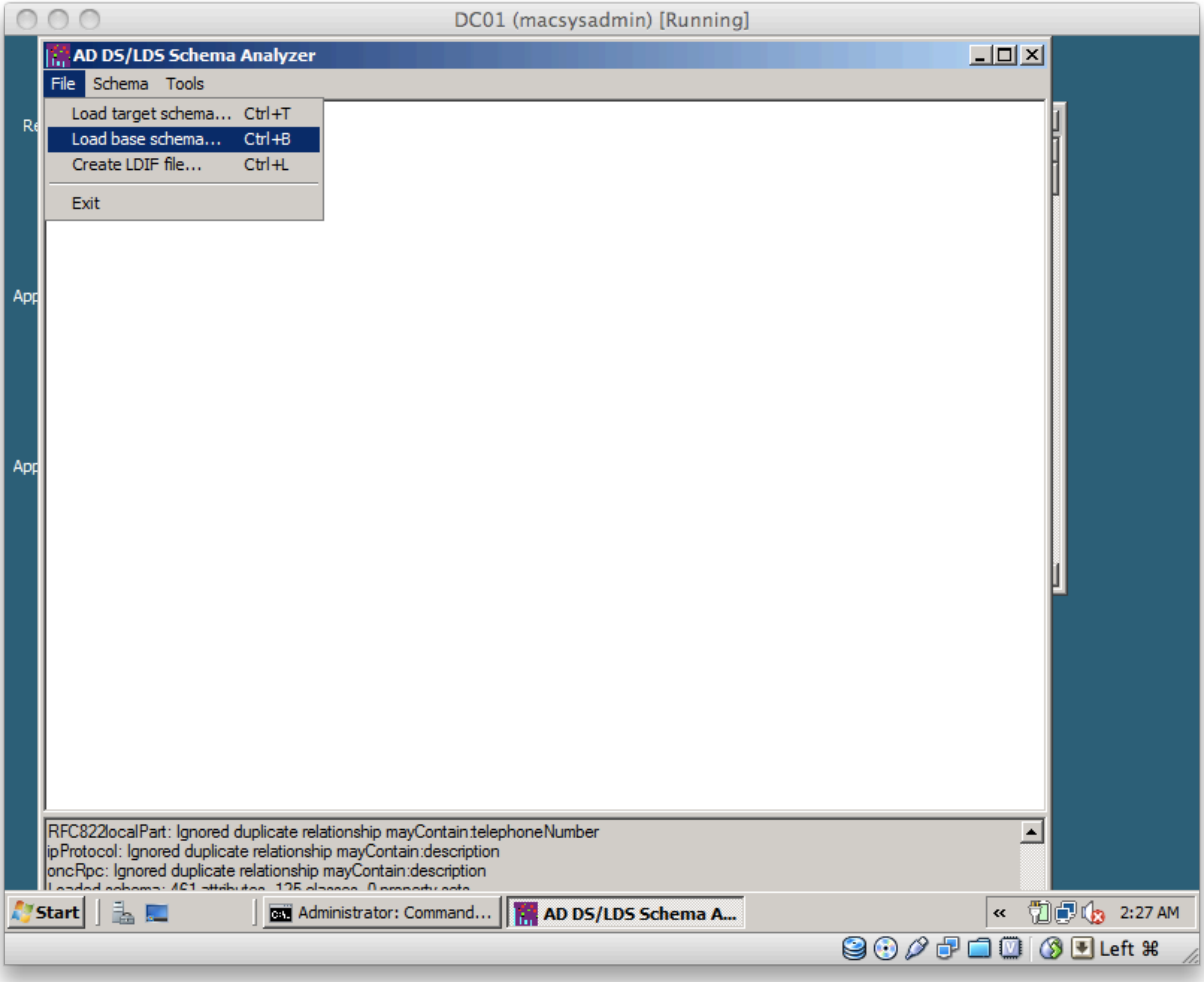
Bind type ○ Secure ● Simple

Server type

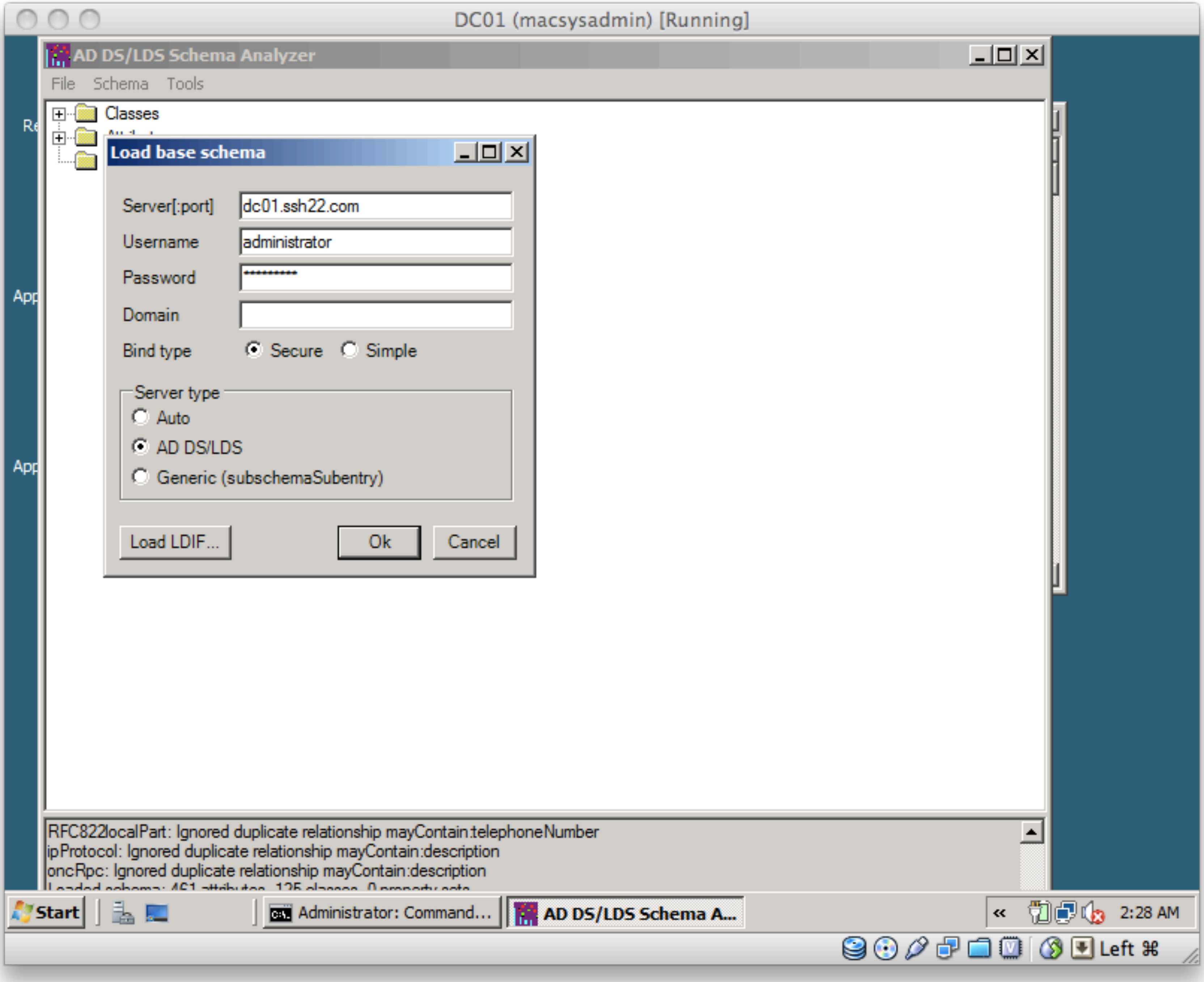
● Auto

○ AD DS/LDS

○ Generic (subschemaSubentry)



```
RFC822localPart: Ignored duplicate relationship mayContain:telephoneNumber
ipProtocol: Ignored duplicate relationship mayContain:description
oncRpc: Ignored duplicate relationship mayContain:description
Loaded schema: 461 attributes, 125 classes, 0 property sets
```



Server[:port] dc01.ssh22.com

Username administrator

Password **********

Domain

Bind type ● Secure ○ Simple

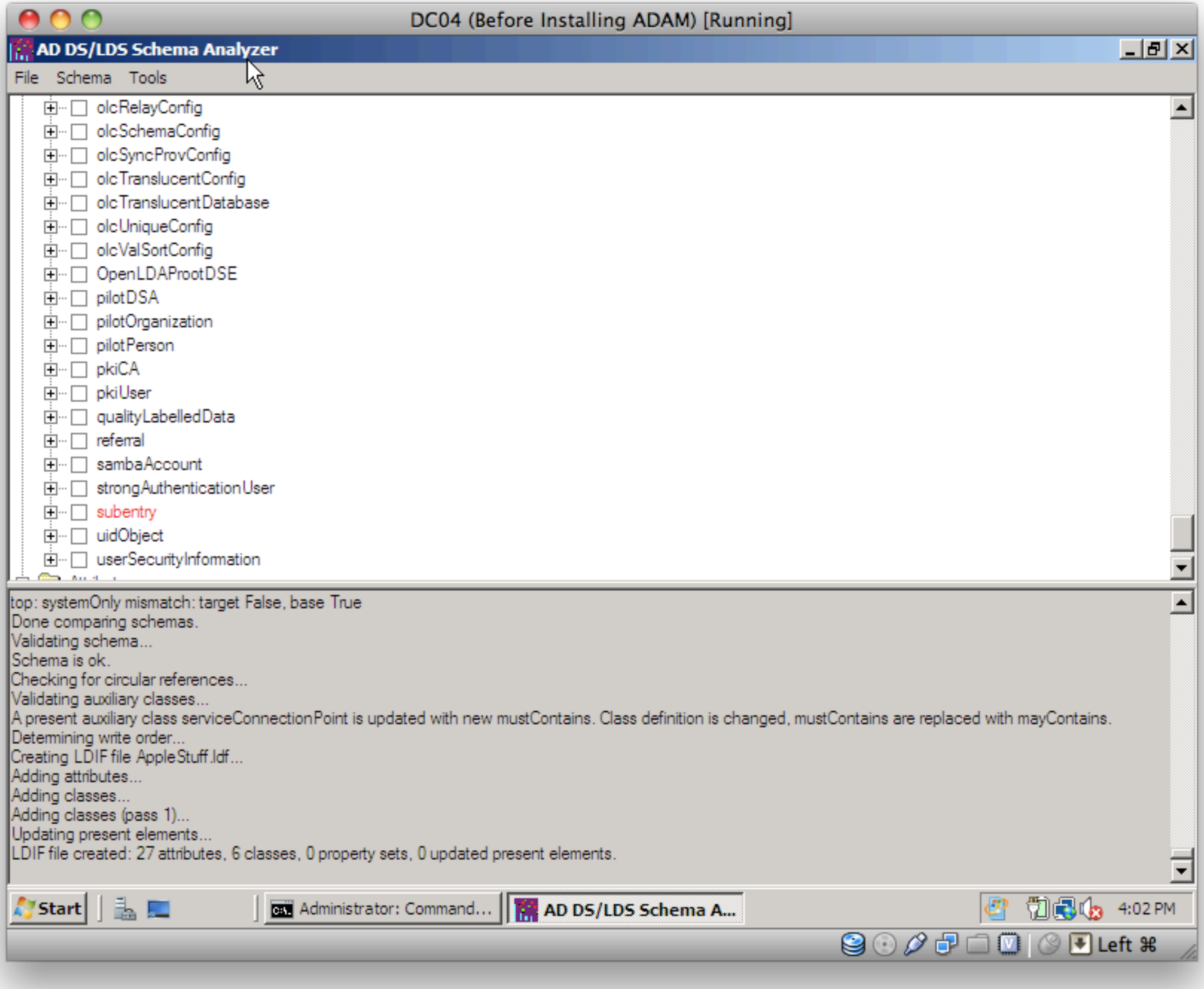
Server type

○ Auto

● AD DS/LDS

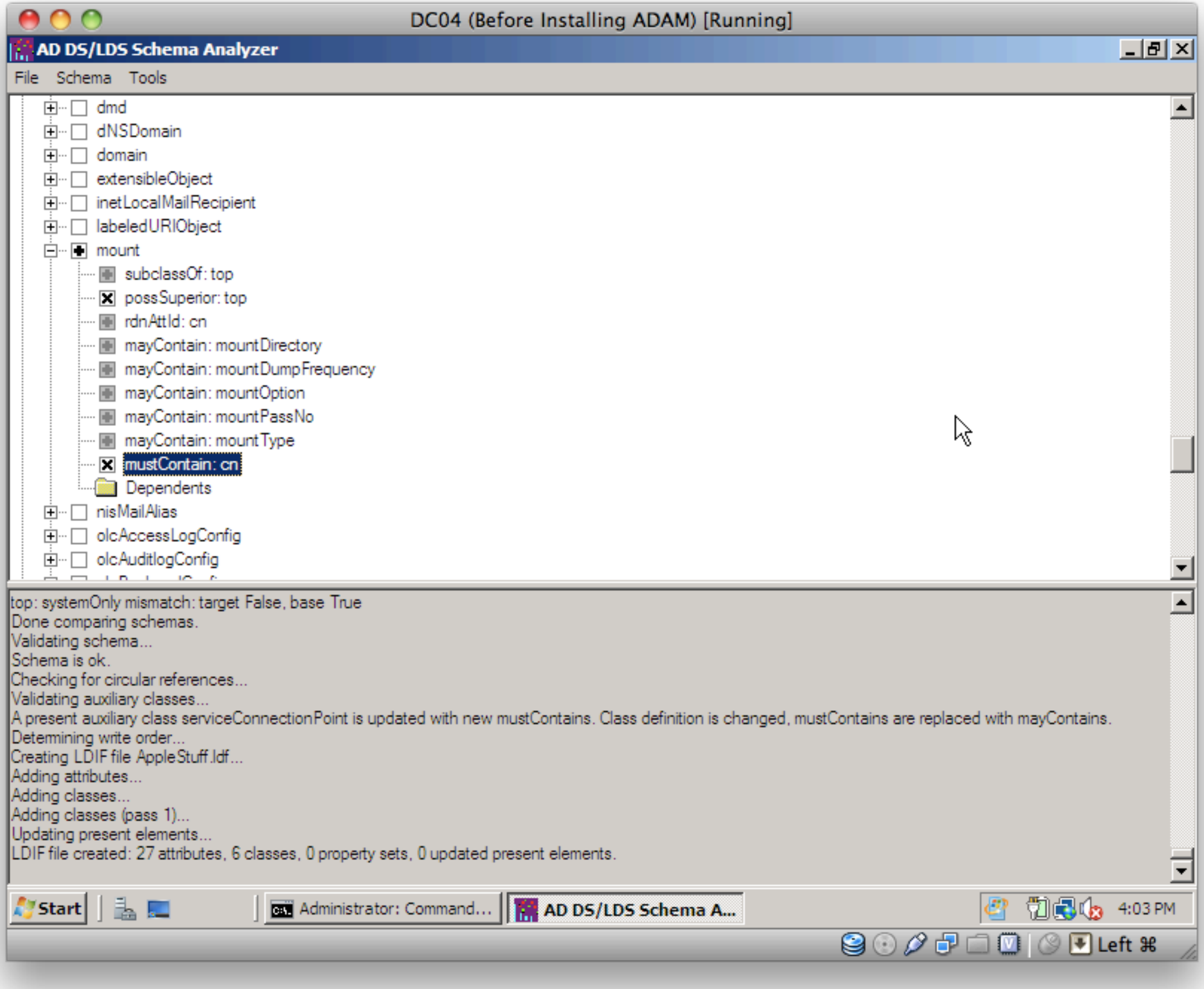
○ Generic (subschemaSubentry)

```
RFC822localPart: Ignored duplicate relationship mayContain:telephoneNumber
ipProtocol: Ignored duplicate relationship mayContain:description
oncRpc: Ignored duplicate relationship mayContain:description
Loaded schema: 461 attributes, 125 classes, 0 property sets
```

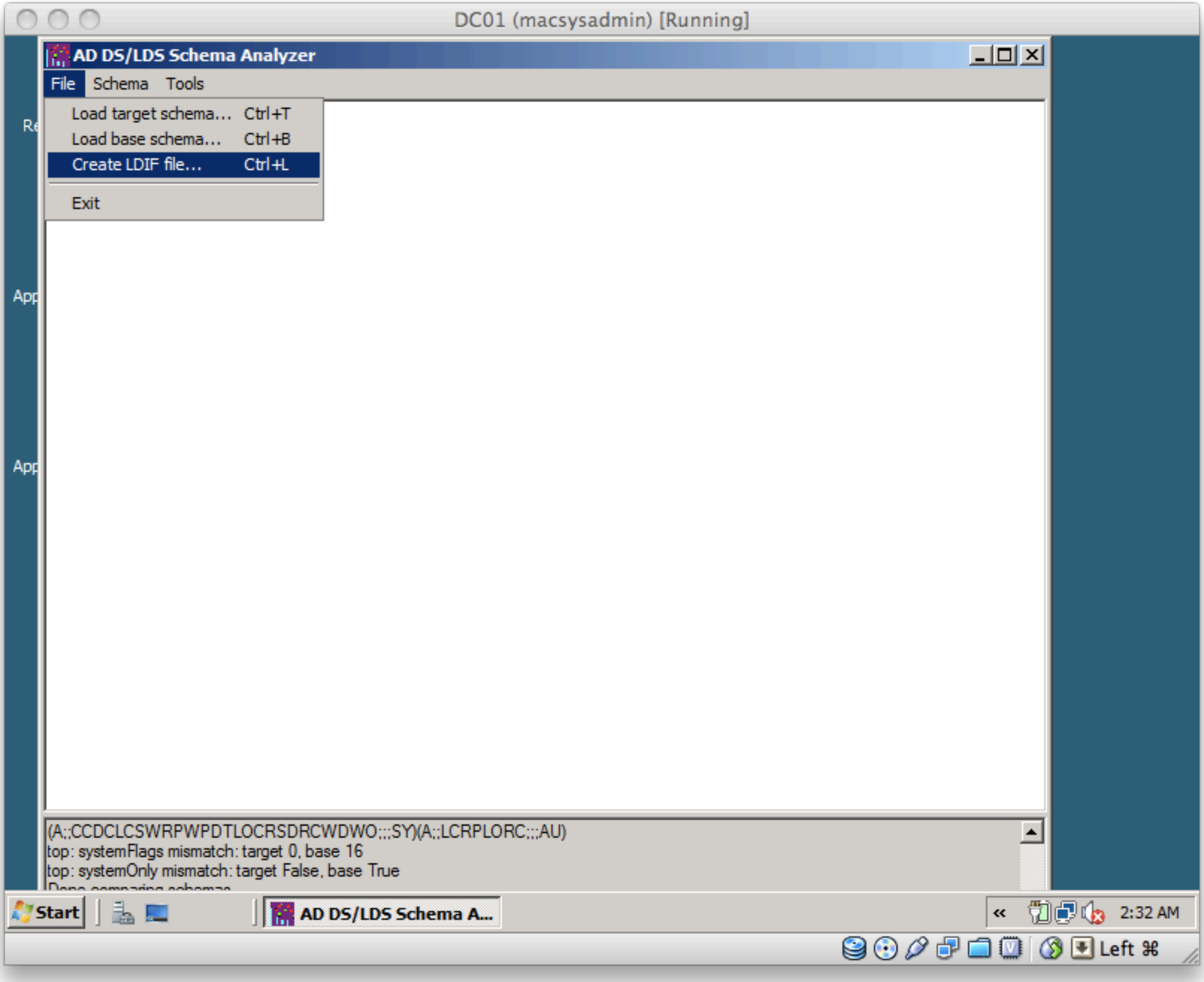

DC04 (Before Installing ADAM) [Running]
AD DS/LDS Schema Analyzer
File
Schema
Tools
Start
Administrator: Command...
AD DS/LDS Schema A...
4:02 PM
Left ⌘

☐ olcRelayConfig
☐ olcSchemaConfig
☐ olcSyncProvConfig
☐ olcTranslucentConfig
☐ olcTranslucentDatabase
☐ olcUniqueConfig
☐ olcValSortConfig
☐ OpenLDAProotDSE
☐ pilotDSA
☐ pilotOrganization
☐ pilotPerson
☐ pkiCA
☐ pkiUser
☐ qualityLabelledData
☐ referral
☐ sambaAccount
☐ strongAuthenticationUser
☐ subentry
☐ uidObject
☐ userSecurityInformation

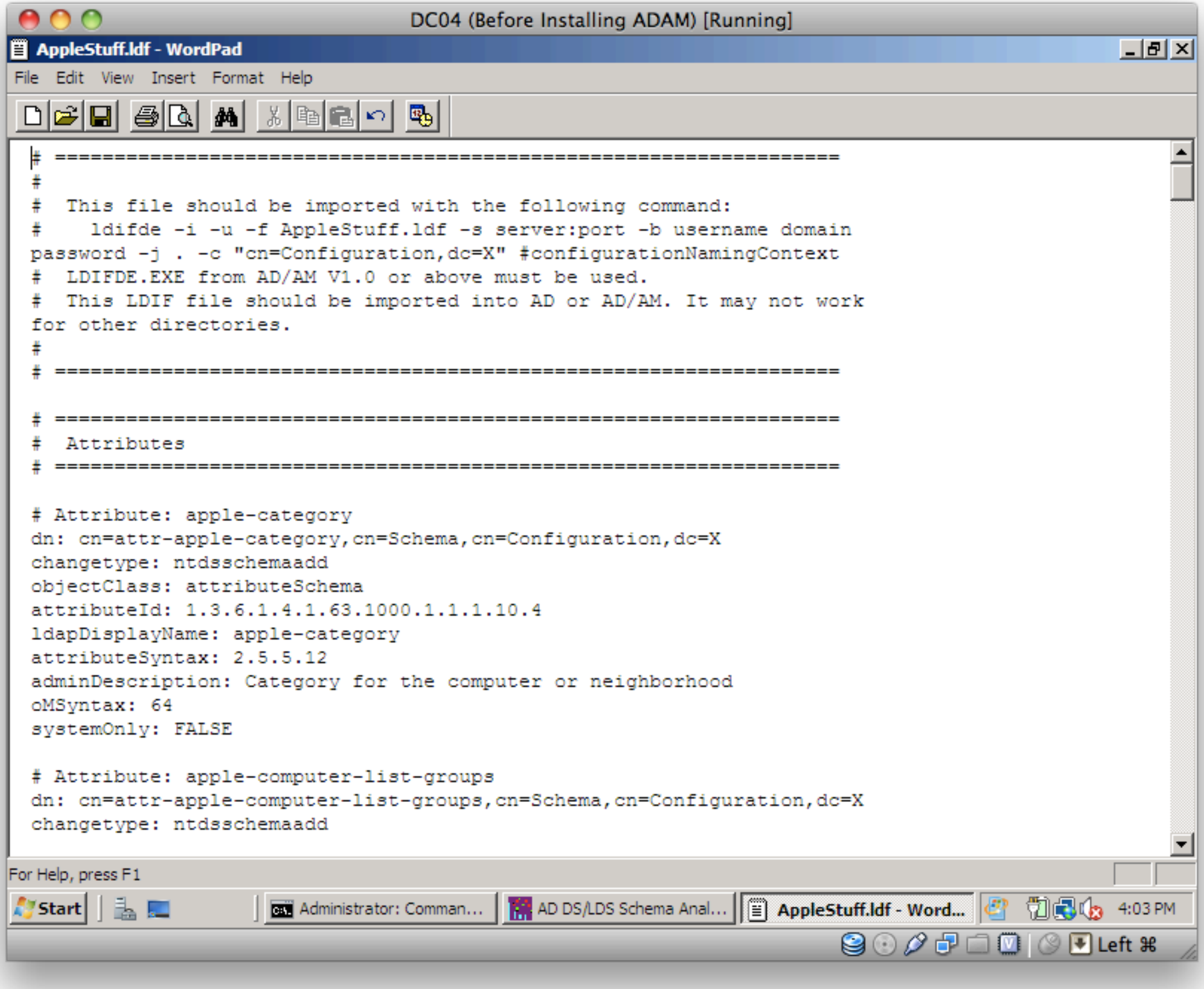
```
top: systemOnly mismatch: target False, base True
Done comparing schemas.
Validating schema...
Schema is ok.
Checking for circular references...
Validating auxiliary classes...
A present auxiliary class serviceConnectionPoint is updated with new mustContains. Class definition is changed, mustContains are replaced with mayContains.
Determining write order...
Creating LDIF file AppleStuff.ldf...
Adding attributes...
Adding classes...
Adding classes (pass 1)...
Updating present elements...
LDIF file created: 27 attributes, 6 classes, 0 property sets, 0 updated present elements.
```



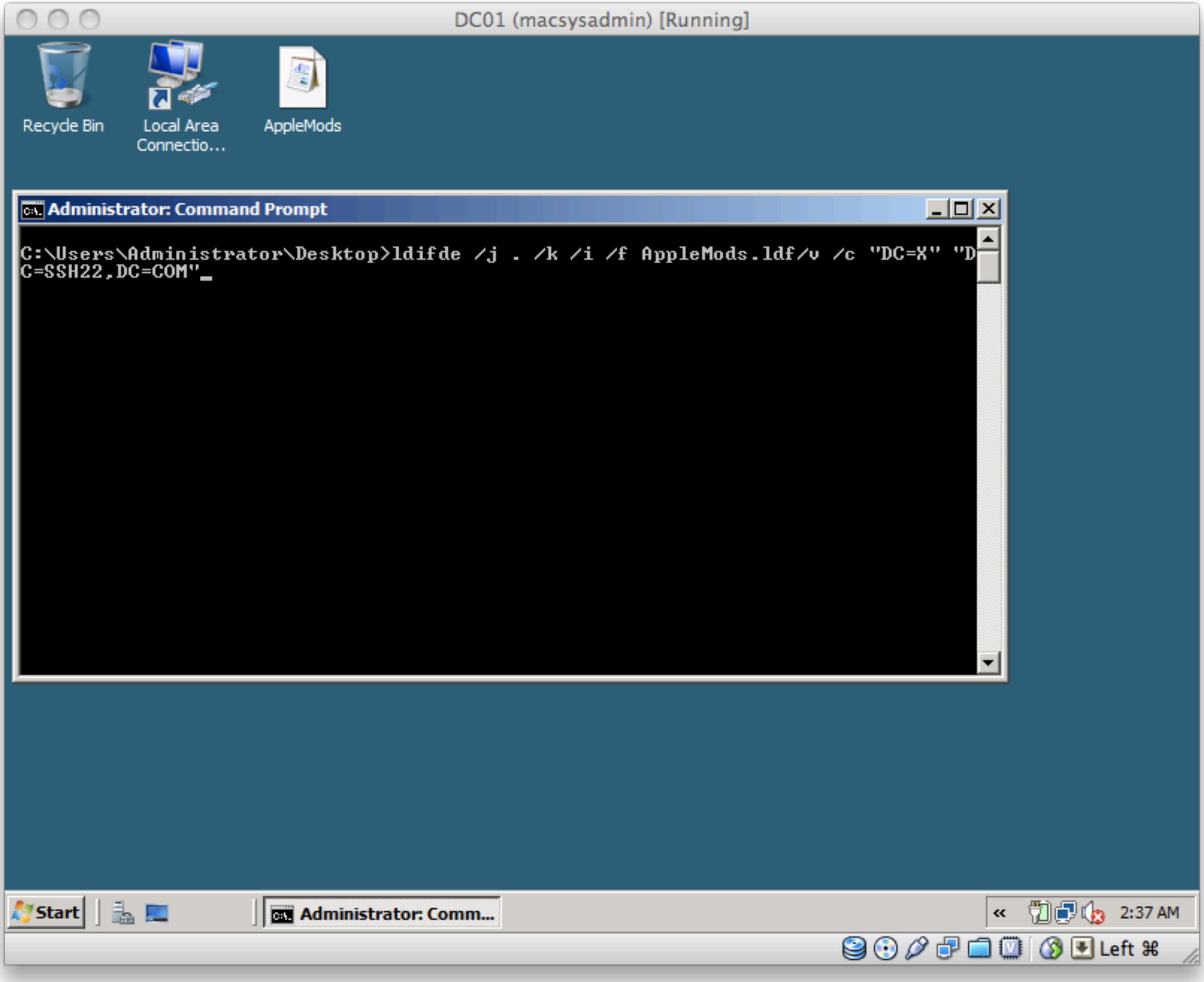
```
top: systemOnly mismatch: target False, base True
Done comparing schemas.
Validating schema...
Schema is ok.
Checking for circular references...
Validating auxiliary classes...
A present auxiliary class serviceConnectionPoint is updated with new mustContains. Class definition is changed, mustContains are replaced with mayContains.
Determining write order...
Creating LDIF file AppleStuff.ldf...
Adding attributes...
Adding classes...
Adding classes (pass 1)...
Updating present elements...
LDIF file created: 27 attributes, 6 classes, 0 property sets, 0 updated present elements.
```


DC01 (macsysadmin) [Running]
AD DS/LDS Schema Analyzer
File
Schema
Tools
Load target schema... Ctrl+T
Load base schema... Ctrl+B
Create LDIF file... Ctrl+L
Exit
Start
AD DS/LDS Schema A...
2:32 AM
Left ⌘

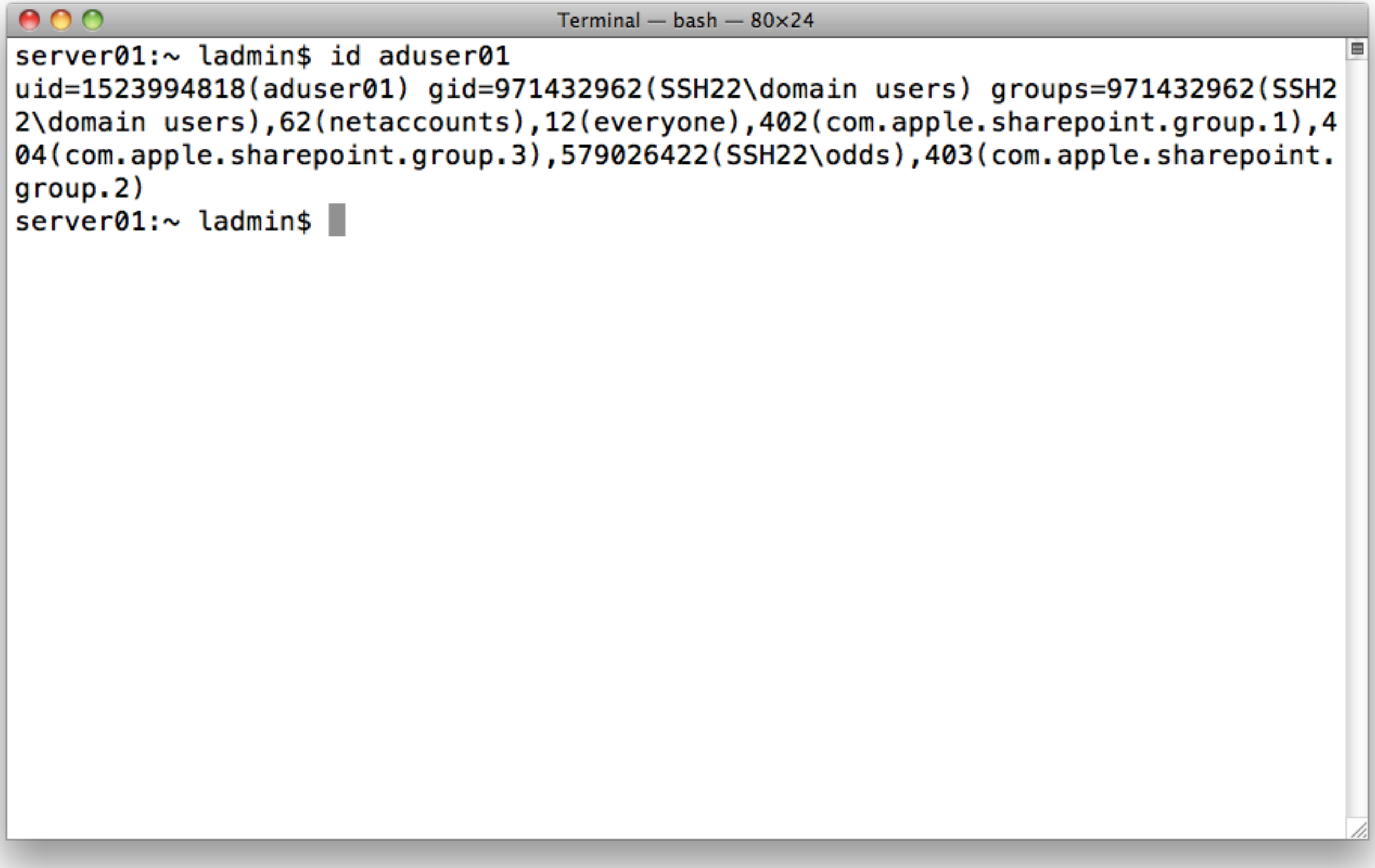
```
(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SY)(A;;LCRPLORC;;;AU)
top: systemFlags mismatch: target 0, base 16
top: systemOnly mismatch: target False, base True
Done comparing schemas
```



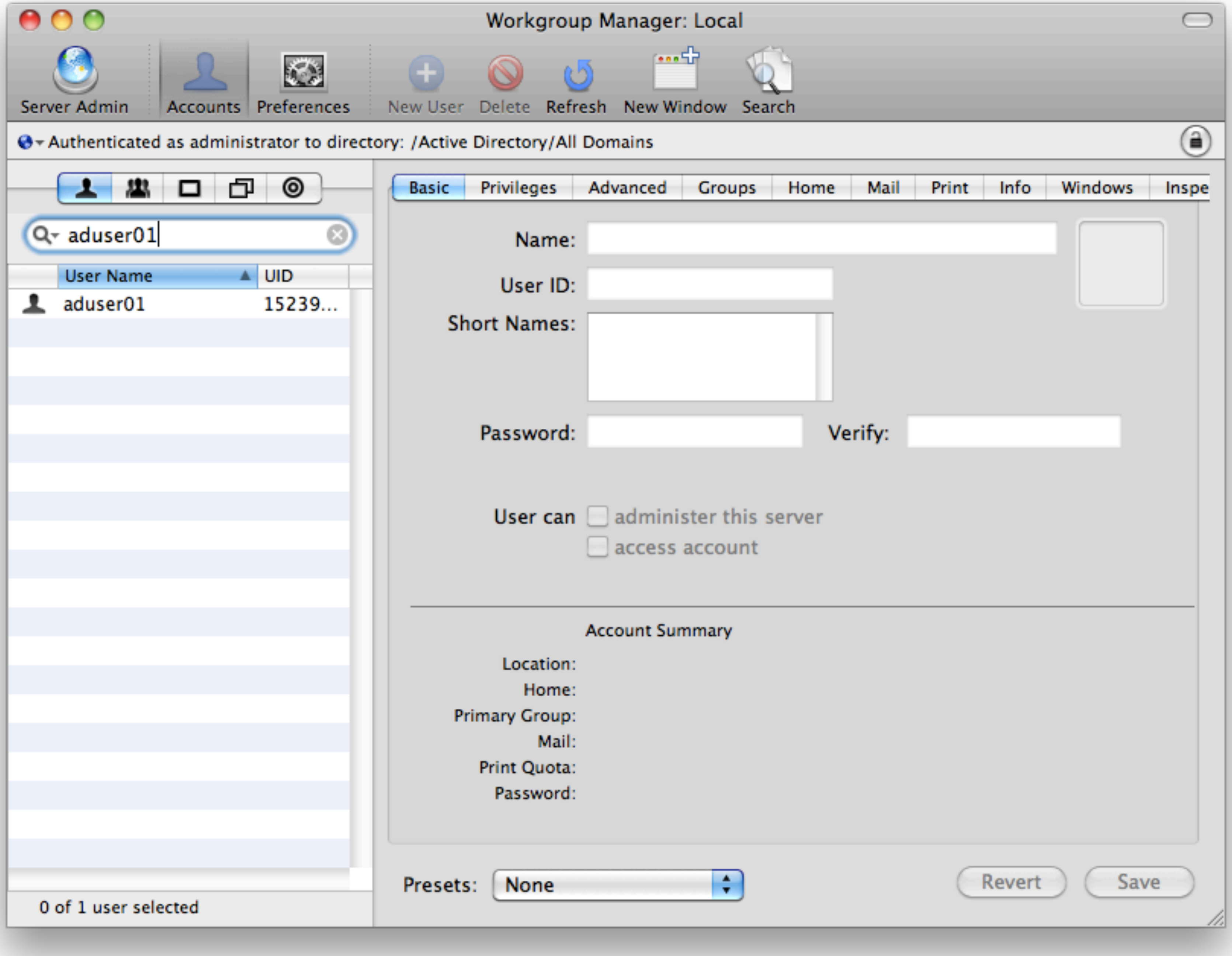
```
# ==================================================================
#
#  This file should be imported with the following command:
#    ldifde -i -u -f AppleStuff.ldf -s server:port -b username domain
password -j . -c "cn=Configuration,dc=X" #configurationNamingContext
#  LDIFDE.EXE from AD/AM V1.0 or above must be used.
#  This LDIF file should be imported into AD or AD/AM. It may not work
for other directories.
#
# ==================================================================

# ==================================================================
#  Attributes
# ==================================================================

# Attribute: apple-category
dn: cn=attr-apple-category,cn=Schema,cn=Configuration,dc=X
changetype: ntdsschemaadd
objectClass: attributeSchema
attributeId: 1.3.6.1.4.1.63.1000.1.1.1.10.4
ldapDisplayName: apple-category
attributeSyntax: 2.5.5.12
adminDescription: Category for the computer or neighborhood
oMSyntax: 64
systemOnly: FALSE

# Attribute: apple-computer-list-groups
dn: cn=attr-apple-computer-list-groups,cn=Schema,cn=Configuration,dc=X
changetype: ntdsschemaadd
```



```
C:\Users\Administrator\Desktop>ldifde /j . /k /i /f AppleMods.ldf/v /c "DC=X" "D
C=SSH22,DC=COM"_
```



```
server01:~ ladmin$ id aduser01
uid=1523994818(aduser01) gid=971432962(SSH22\domain users) groups=971432962(SSH2
2\domain users),62(netaccounts),12(everyone),402(com.apple.sharepoint.group.1),4
04(com.apple.sharepoint.group.3),579026422(SSH22\odds),403(com.apple.sharepoint.
group.2)
server01:~ ladmin$ 
```



Authenticated as administrator to directory: /Active Directory/All Domains

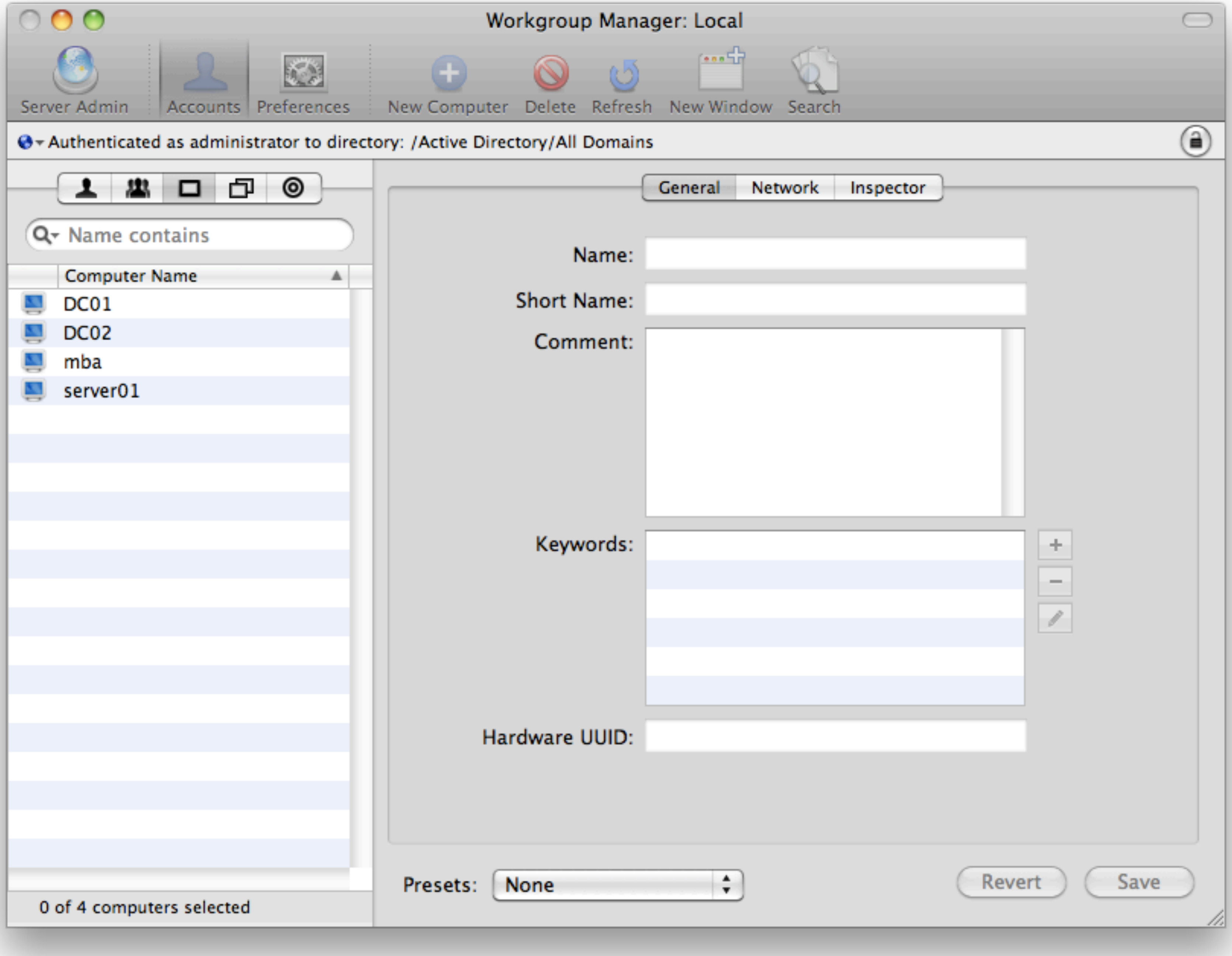
aduser01

User Name	UID
aduser01	15239...

0 of 1 user selected

User can □ administer this server
□ access account

Presets: None



Workgroup Manager: Local

Authenticated as administrator to directory: /Active Directory/All Domains

Computer Name

DC01
DC02
mba
server01

0 of 4 computers selected

Name:

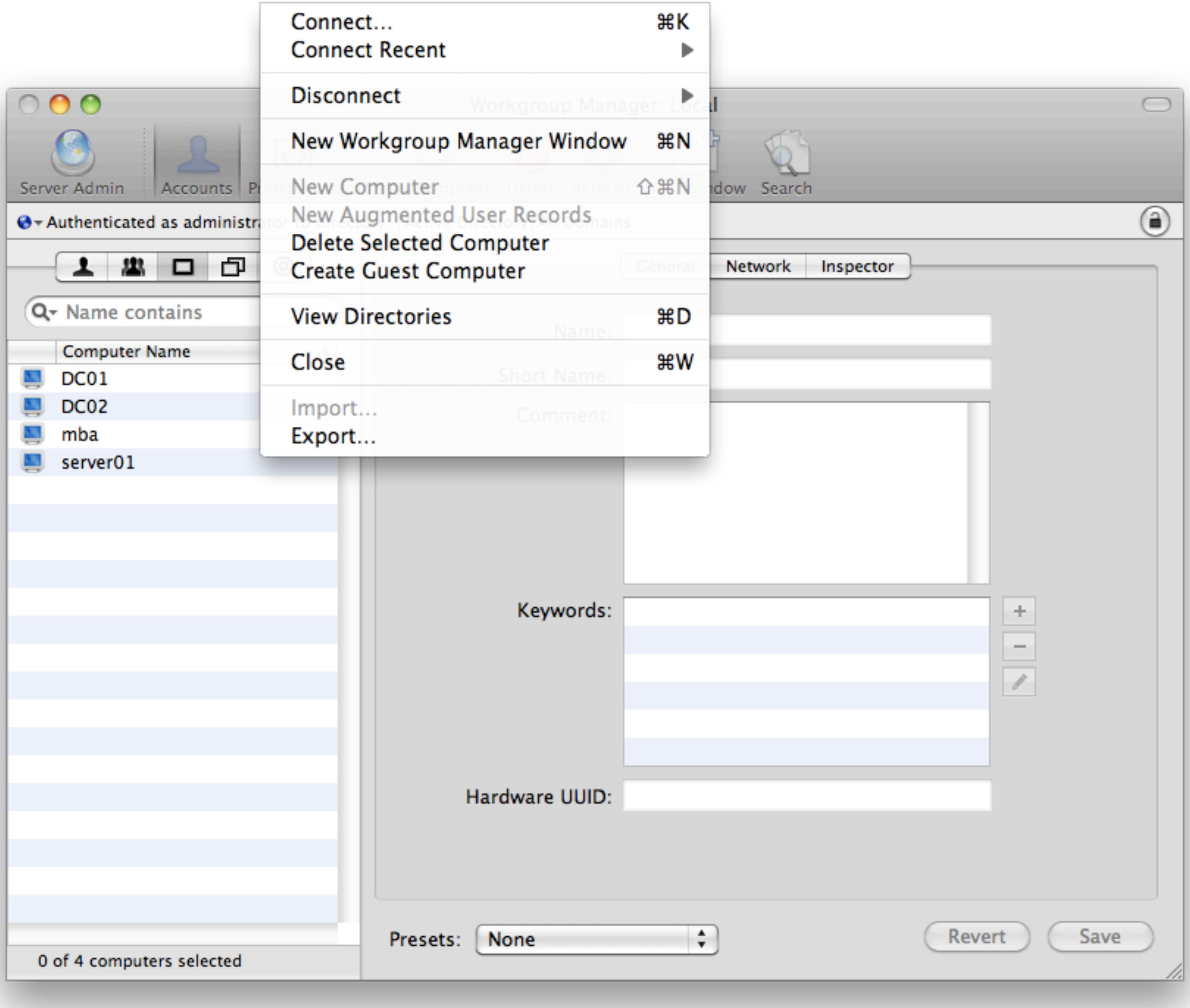
Short Name:

Comment:

Keywords:

Hardware UUID:

Presets: None

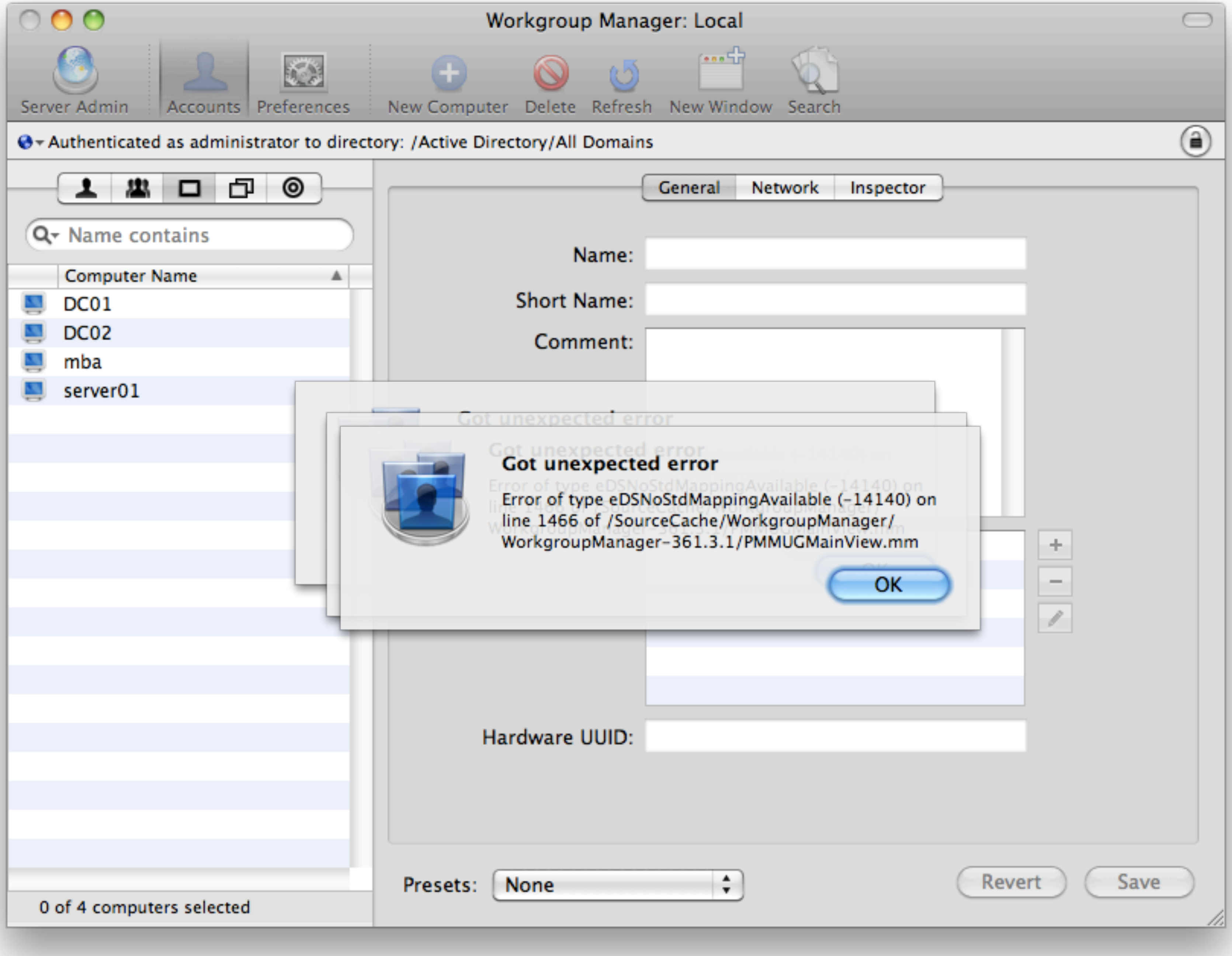


Authenticated as administrator

Computer Name
DC01
DC02
mba
server01

0 of 4 computers selected

Presets: None



Authenticated as administrator to directory: /Active Directory/All Domains

Name:

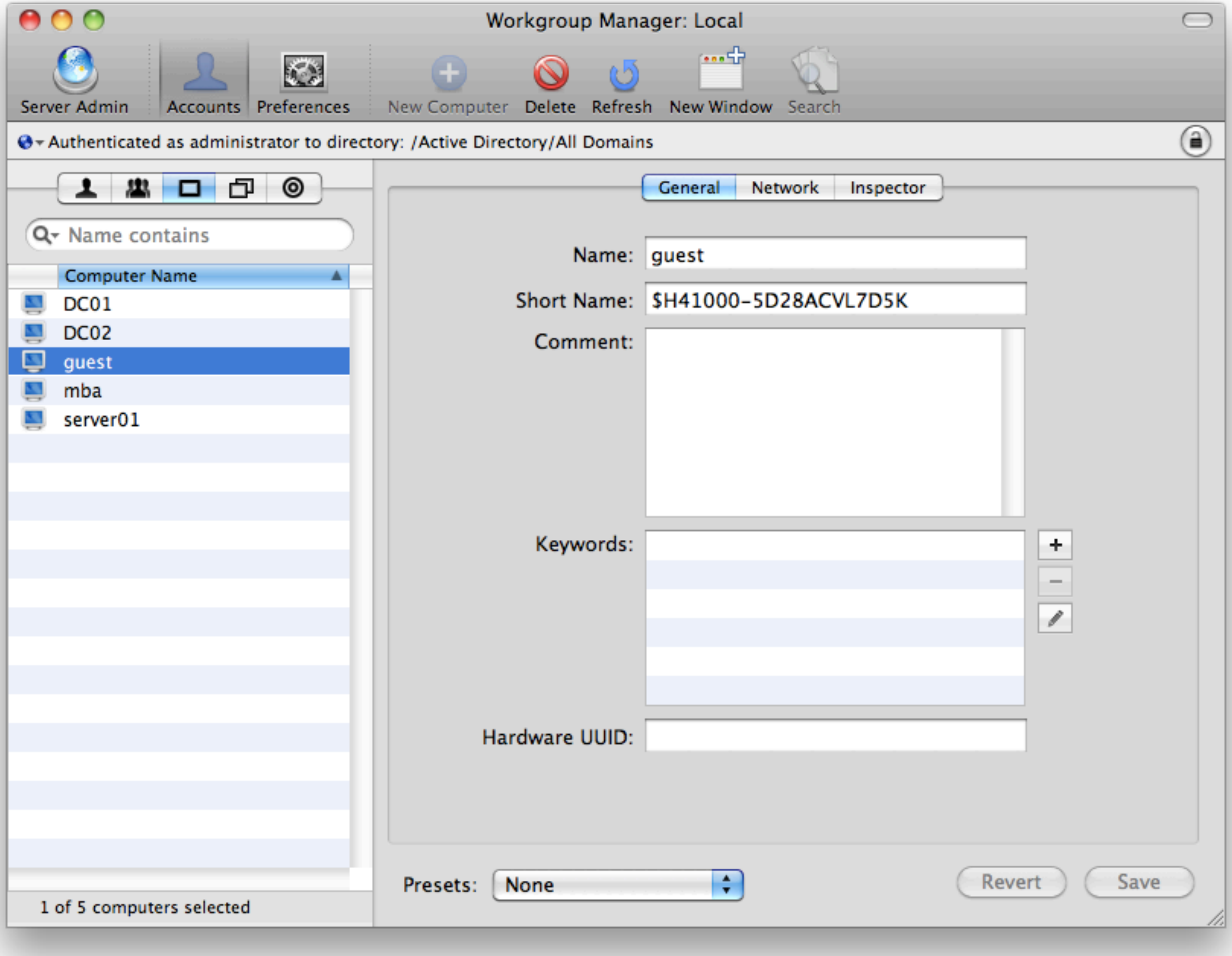
Short Name:

Comment:

Hardware UUID:

Got unexpected error

Error of type eDSNoStdMappingAvailable (-14140) on line 1466 of /SourceCache/WorkgroupManager/WorkgroupManager-361.3.1/PMMUGMainView.mm



Authenticated as administrator to directory: /Active Directory/All Domains

DC01
DC02
guest
mba
server01

1 of 5 computers selected

Name: guest

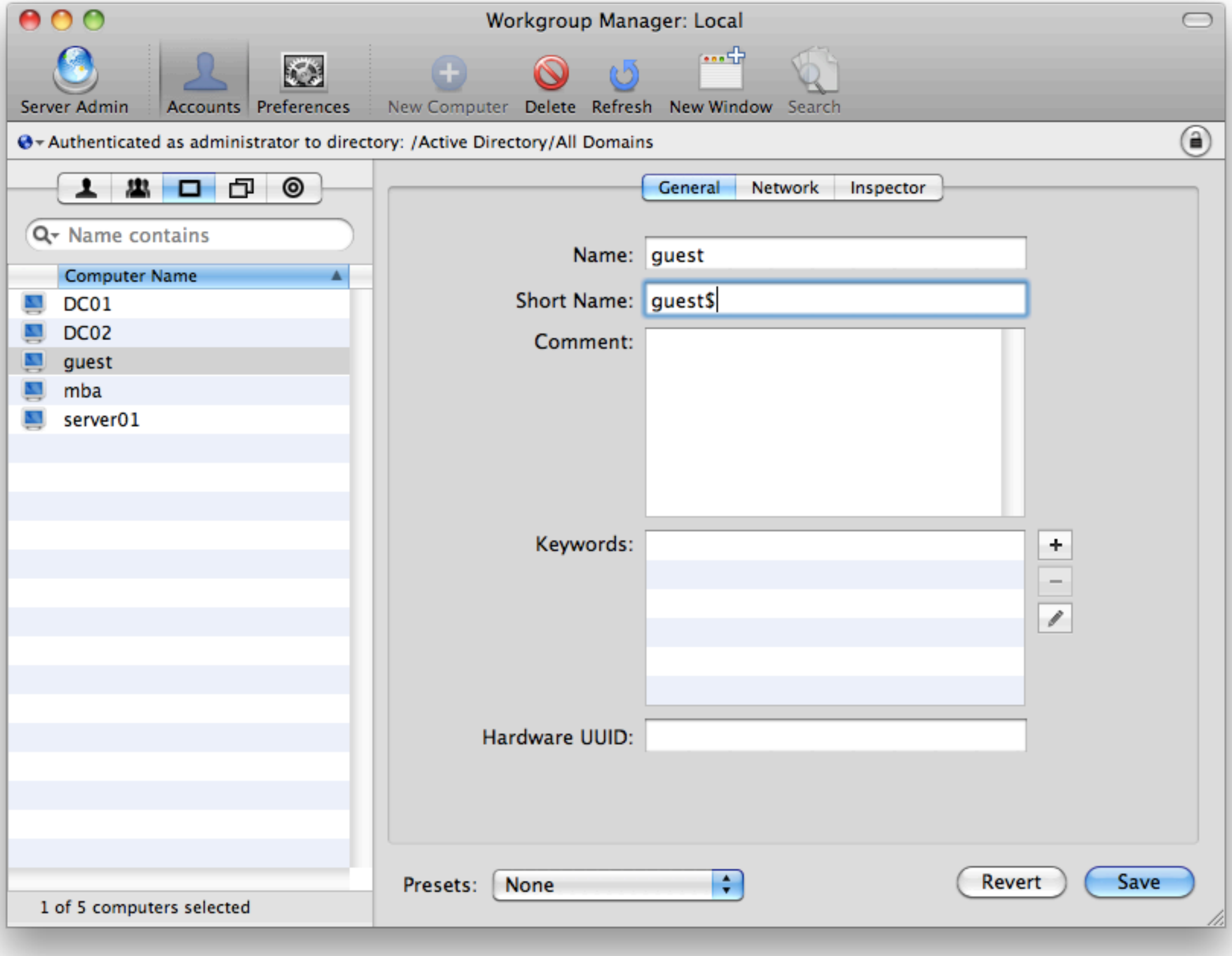
Short Name: $H41000-5D28ACVL7D5K

Comment:

Keywords:

Hardware UUID:

Presets: None



Workgroup Manager: Local

Authenticated as administrator to directory: /Active Directory/All Domains

Computer Name
DC01
DC02
guest
mba
server01

1 of 5 computers selected

Name: guest

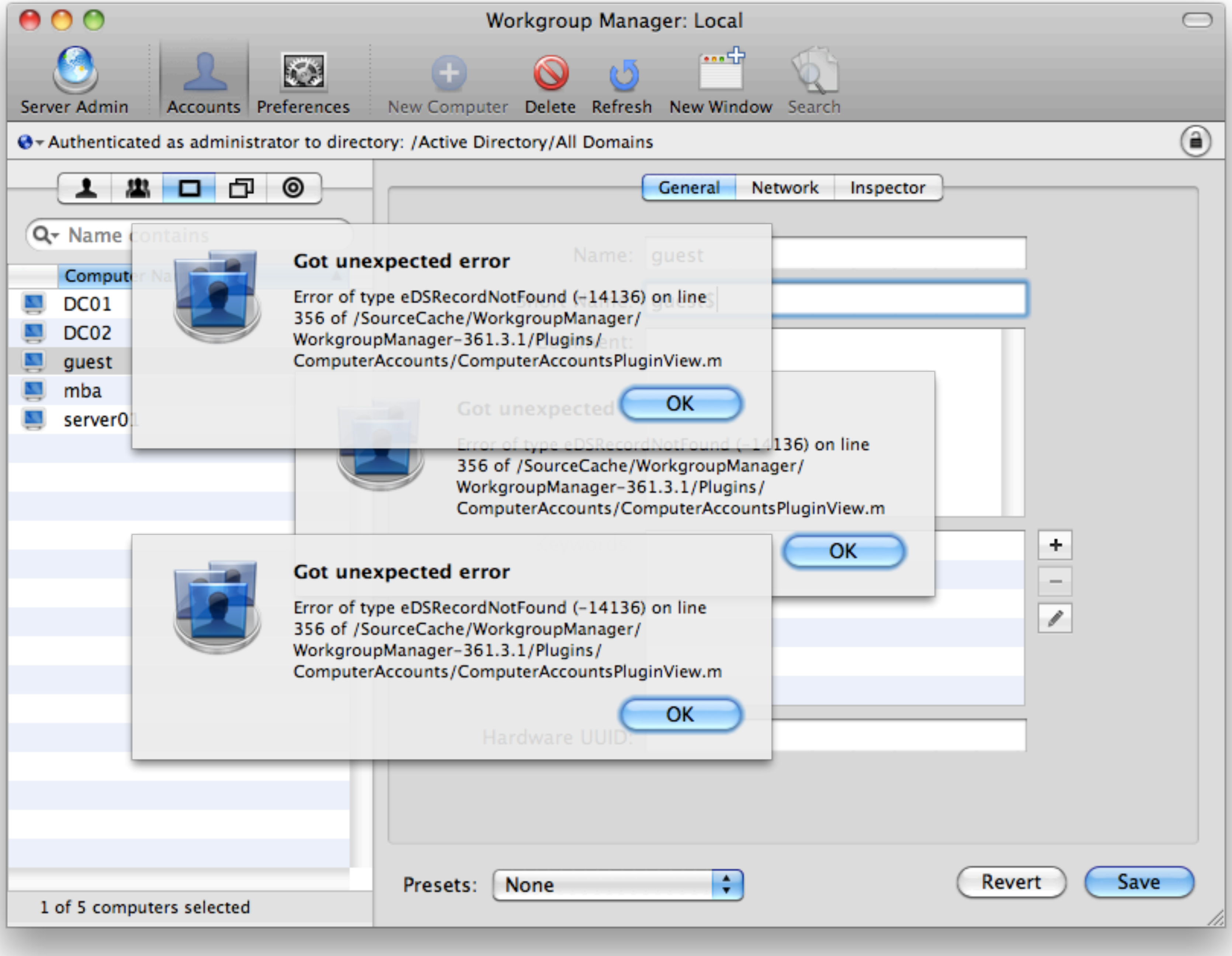
Short Name: guest$

Comment:

Keywords:

Hardware UUID:

Presets: None



Authenticated as administrator to directory: /Active Directory/All Domains

Name: guest

Got unexpected error

Error of type eDSRecordNotFound (-14136) on line 356 of /SourceCache/WorkgroupManager/WorkgroupManager-361.3.1/Plugins/ComputerAccounts/ComputerAccountsPluginView.m

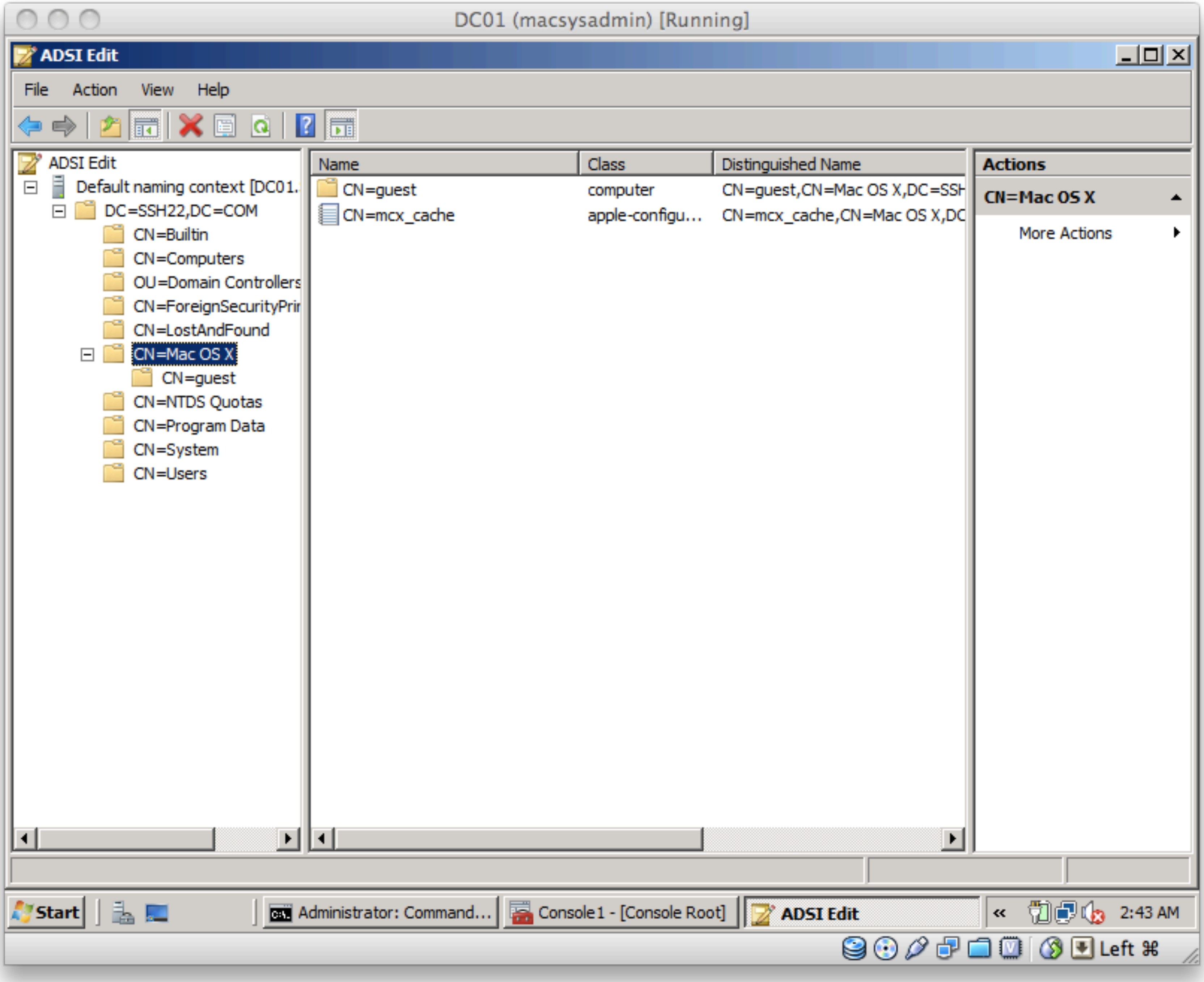
Got unexpected error

Error of type eDSRecordNotFound (-14136) on line 356 of /SourceCache/WorkgroupManager/WorkgroupManager-361.3.1/Plugins/ComputerAccounts/ComputerAccountsPluginView.m

Got unexpected error

Error of type eDSRecordNotFound (-14136) on line 356 of /SourceCache/WorkgroupManager/WorkgroupManager-361.3.1/Plugins/ComputerAccounts/ComputerAccountsPluginView.m

1 of 5 computers selected



```
ADSI Edit
⊟ Default naming context [DC01.
   ⊟ DC=SSH22,DC=COM
        CN=Builtin
        CN=Computers
        OU=Domain Controllers
        CN=ForeignSecurityPrir
        CN=LostAndFound
      ⊟ CN=Mac OS X
           CN=guest
        CN=NTDS Quotas
        CN=Program Data
        CN=System
        CN=Users
```

Name	Class	Distinguished Name
CN=guest	computer	CN=guest,CN=Mac OS X,DC=SSH
CN=mcx_cache	apple-configu...	CN=mcx_cache,CN=Mac OS X,DC

Why NOT Extend

- Reluctance from *some* at Apple
- AD admins still afraid
  - especially with older Windows server
- Computer Lists (not Computer Groups)

3: Dual Directory

- Pretty well known and documented

4: Third Party

- DFS
- Support
- Centralized Management of all objects
- ALL clients must participate

DFS

- DFS is a great idea...theoretically
- Hacks to enable DFS access
    - not so great for home folders

Support

- One point of contact

Central Management

- AD Administrator defines policies for all
- Mac Administrator often out of picture

Money

- Must purchase for EVERY Mac
- User ID calculated differently

4 Strategies: Review

- Bind to AD only
- Bind to AD and extend AD
- Dual Directory
- Third-party

Challenges Addressed?

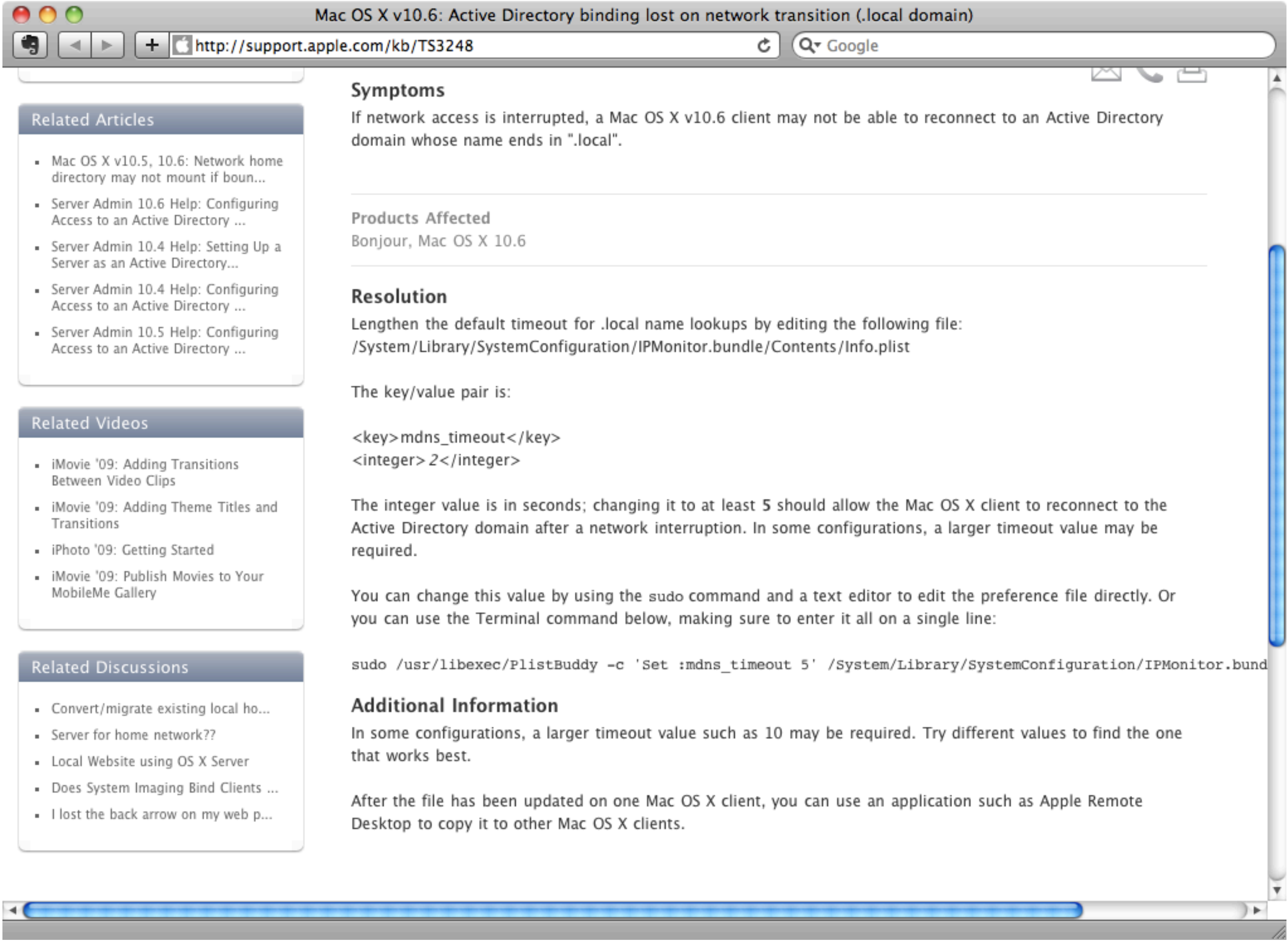
- Managed Preferences for Apple objects
- Accessing DFS Shares

15 Issues with AD

- 12 Knowledge Base articles
- 3 Real-world edge cases

12 KBs

- Specific to Active Directory integration


Mac OS X v10.6: Active Directory binding lost on network transition (.local domain)
http://support.apple.com/kb/TS3248
Google

Related Articles

- Mac OS X v10.5, 10.6: Network home directory may not mount if boun...
- Server Admin 10.6 Help: Configuring Access to an Active Directory ...
- Server Admin 10.4 Help: Setting Up a Server as an Active Directory...
- Server Admin 10.4 Help: Configuring Access to an Active Directory ...
- Server Admin 10.5 Help: Configuring Access to an Active Directory ...

Related Videos

- iMovie '09: Adding Transitions Between Video Clips
- iMovie '09: Adding Theme Titles and Transitions
- iPhoto '09: Getting Started
- iMovie '09: Publish Movies to Your MobileMe Gallery

Related Discussions

- Convert/migrate existing local ho...
- Server for home network??
- Local Website using OS X Server
- Does System Imaging Bind Clients ...
- I lost the back arrow on my web p...

Symptoms

If network access is interrupted, a Mac OS X v10.6 client may not be able to reconnect to an Active Directory domain whose name ends in ".local".

Products Affected

Bonjour, Mac OS X 10.6

Resolution

Lengthen the default timeout for .local name lookups by editing the following file:
/System/Library/SystemConfiguration/IPMonitor.bundle/Contents/Info.plist

The key/value pair is:

```
<key>mdns_timeout</key>
<integer>2</integer>
```

The integer value is in seconds; changing it to at least **5** should allow the Mac OS X client to reconnect to the Active Directory domain after a network interruption. In some configurations, a larger timeout value may be required.

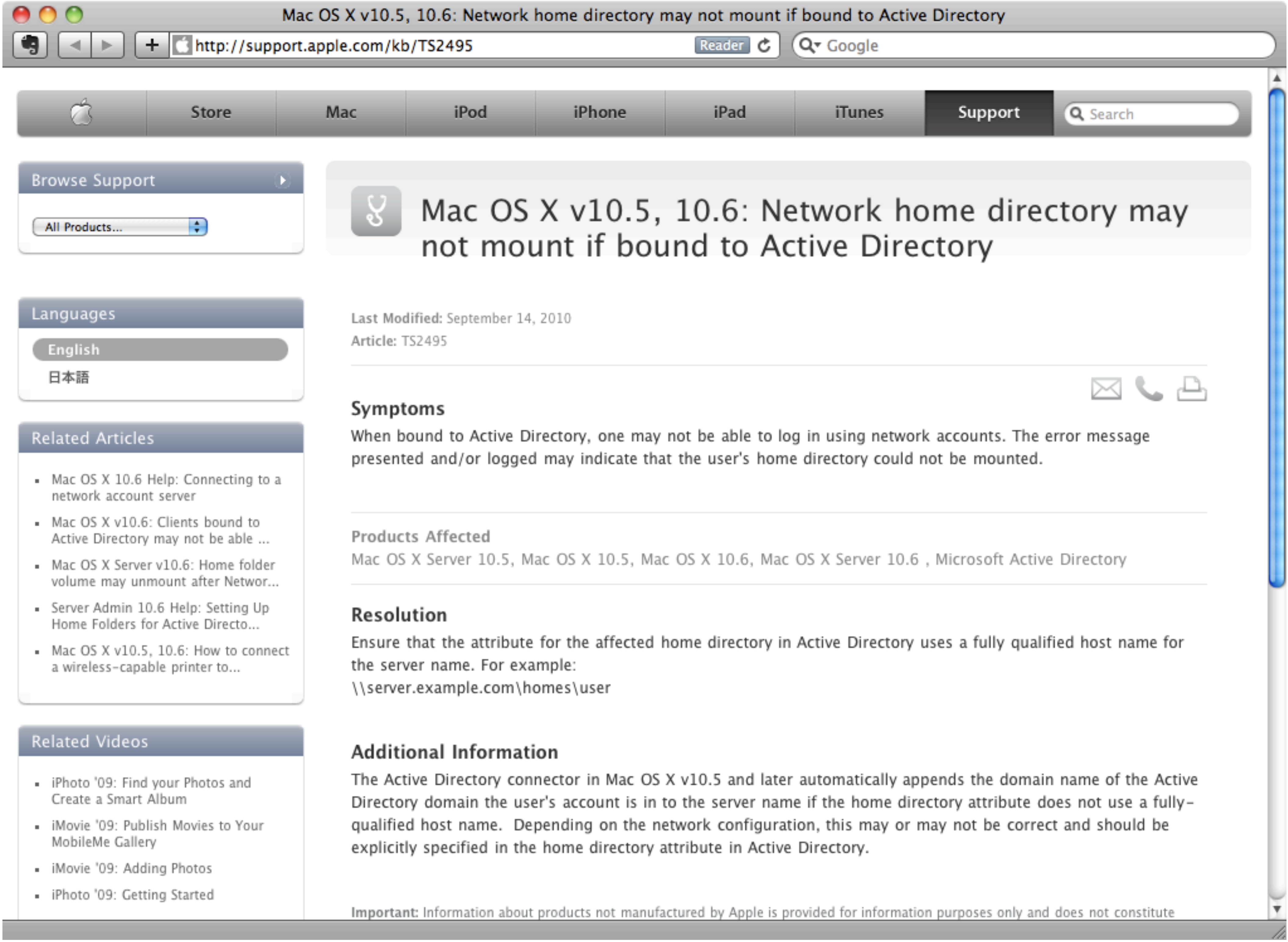
You can change this value by using the sudo command and a text editor to edit the preference file directly. Or you can use the Terminal command below, making sure to enter it all on a single line:

```
sudo /usr/libexec/PlistBuddy -c 'Set :mdns_timeout 5' /System/Library/SystemConfiguration/IPMonitor.bund
```

Additional Information

In some configurations, a larger timeout value such as 10 may be required. Try different values to find the one that works best.

After the file has been updated on one Mac OS X client, you can use an application such as Apple Remote Desktop to copy it to other Mac OS X clients.


Mac OS X v10.5, 10.6: Network home directory may not mount if bound to Active Directory
http://support.apple.com/kb/TS2495
Reader
Google
Store
Mac
iPod
iPhone
iPad
iTunes
Support
Search
Browse Support
All Products...
Languages
English
日本語

Mac OS X v10.5, 10.6: Network home directory may not mount if bound to Active Directory

Last Modified: September 14, 2010

Article: TS2495

Symptoms

When bound to Active Directory, one may not be able to log in using network accounts. The error message presented and/or logged may indicate that the user's home directory could not be mounted.

Products Affected

Mac OS X Server 10.5, Mac OS X 10.5, Mac OS X 10.6, Mac OS X Server 10.6 , Microsoft Active Directory

Resolution

Ensure that the attribute for the affected home directory in Active Directory uses a fully qualified host name for the server name. For example:

\\server.example.com\homes\user

Additional Information

The Active Directory connector in Mac OS X v10.5 and later automatically appends the domain name of the Active Directory domain the user's account is in to the server name if the home directory attribute does not use a fully-qualified host name. Depending on the network configuration, this may or may not be correct and should be explicitly specified in the home directory attribute in Active Directory.

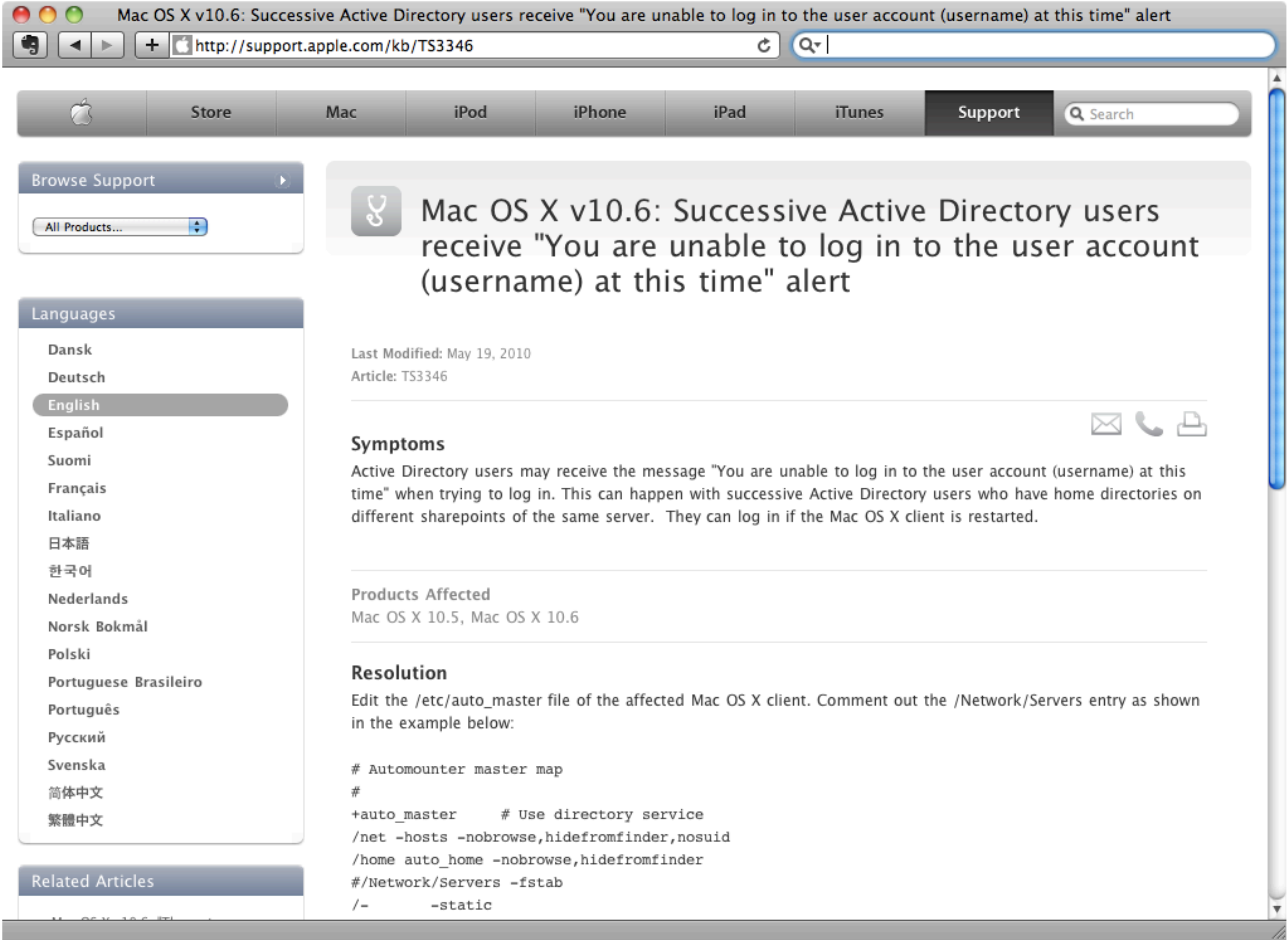
Important: Information about products not manufactured by Apple is provided for information purposes only and does not constitute

Related Articles

- Mac OS X 10.6 Help: Connecting to a network account server
- Mac OS X v10.6: Clients bound to Active Directory may not be able ...
- Mac OS X Server v10.6: Home folder volume may unmount after Networ...
- Server Admin 10.6 Help: Setting Up Home Folders for Active Directo...
- Mac OS X v10.5, 10.6: How to connect a wireless-capable printer to...

Related Videos

- iPhoto '09: Find your Photos and Create a Smart Album
- iMovie '09: Publish Movies to Your MobileMe Gallery
- iMovie '09: Adding Photos
- iPhoto '09: Getting Started



Mac OS X v10.6: Successive Active Directory users receive "You are unable to log in to the user account (username) at this time" alert

Last Modified: May 19, 2010

Article: TS3346

Symptoms

Active Directory users may receive the message "You are unable to log in to the user account (username) at this time" when trying to log in. This can happen with successive Active Directory users who have home directories on different sharepoints of the same server. They can log in if the Mac OS X client is restarted.

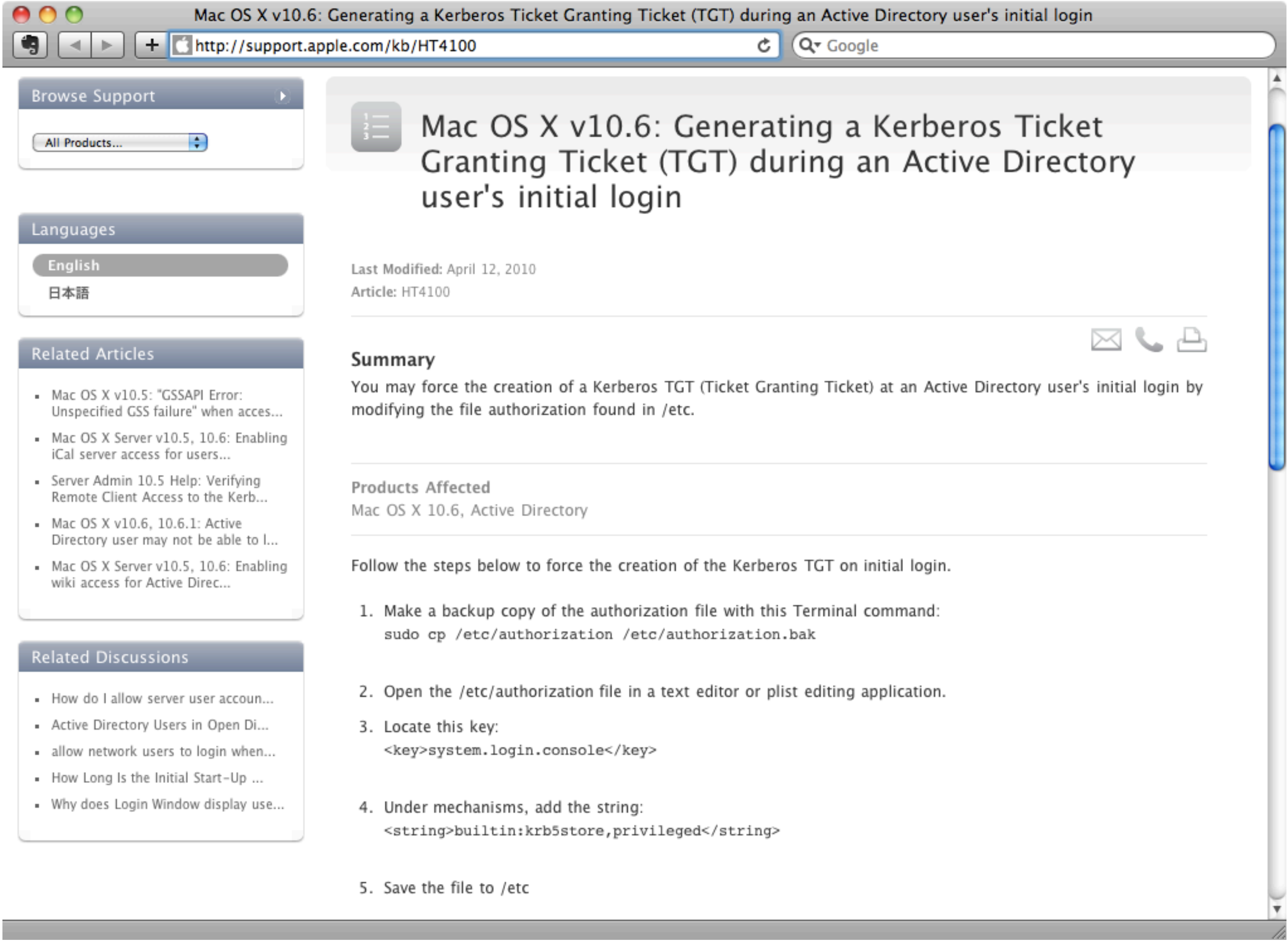
Products Affected

Mac OS X 10.5, Mac OS X 10.6

Resolution

Edit the /etc/auto_master file of the affected Mac OS X client. Comment out the /Network/Servers entry as shown in the example below:

```
# Automounter master map
#
+auto_master     # Use directory service
/net -hosts -nobrowse,hidefromfinder,nosuid
/home auto_home -nobrowse,hidefromfinder
#/Network/Servers -fstab
/-        -static
```


Mac OS X v10.6: Generating a Kerberos Ticket Granting Ticket (TGT) during an Active Directory user's initial login
http://support.apple.com/kb/HT4100
Google
Browse Support
All Products...
Languages
English
日本語
Related Articles
Mac OS X v10.5: "GSSAPI Error: Unspecified GSS failure" when acces...
Mac OS X Server v10.5, 10.6: Enabling iCal server access for users...
Server Admin 10.5 Help: Verifying Remote Client Access to the Kerb...
Mac OS X v10.6, 10.6.1: Active Directory user may not be able to l...
Mac OS X Server v10.5, 10.6: Enabling wiki access for Active Direc...
Related Discussions
How do I allow server user accoun...
Active Directory Users in Open Di...
allow network users to login when...
How Long Is the Initial Start-Up ...
Why does Login Window display use...

Mac OS X v10.6: Generating a Kerberos Ticket Granting Ticket (TGT) during an Active Directory user's initial login

Last Modified: April 12, 2010

Article: HT4100

Summary

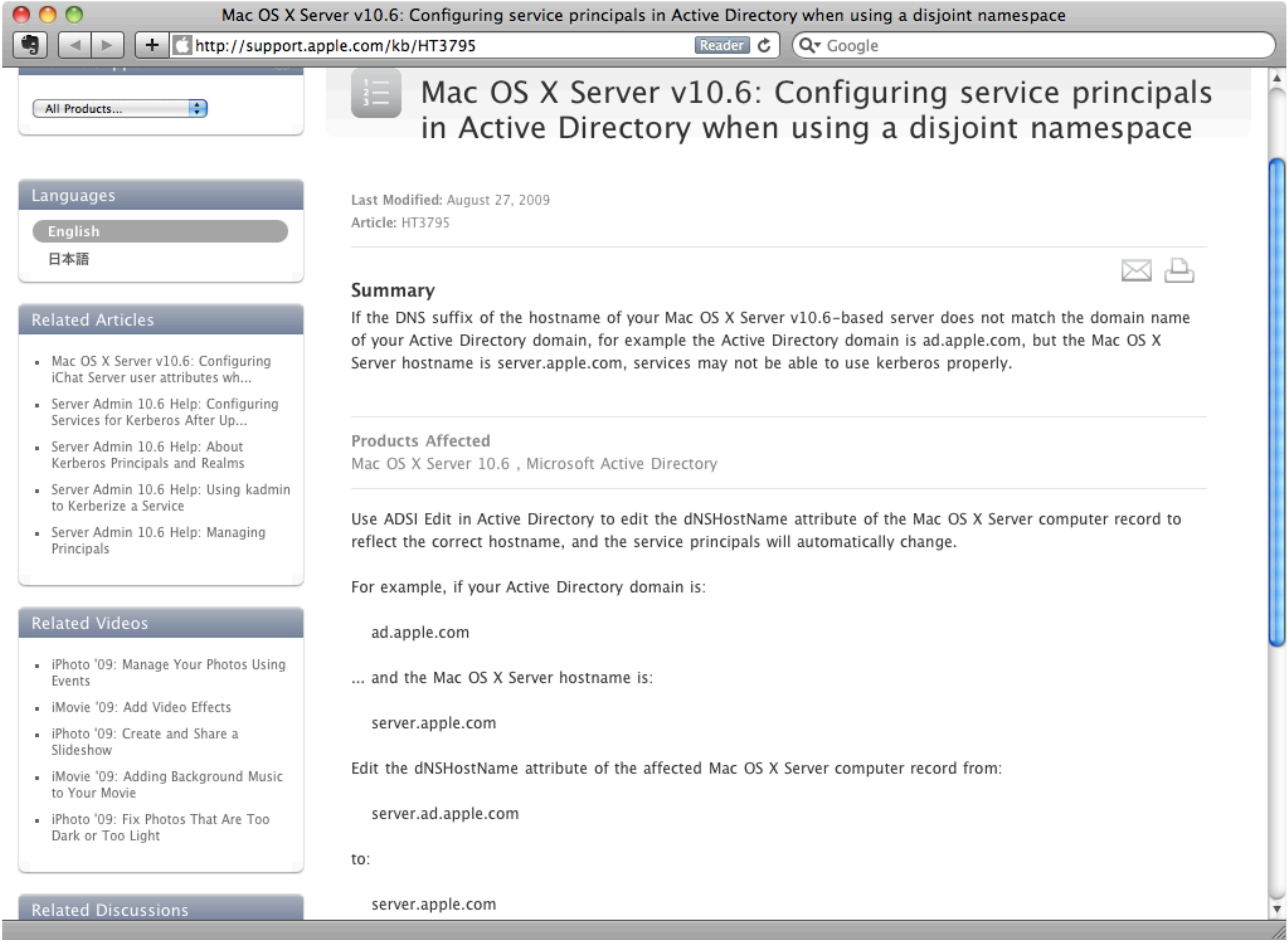
You may force the creation of a Kerberos TGT (Ticket Granting Ticket) at an Active Directory user's initial login by modifying the file authorization found in /etc.

Products Affected

Mac OS X 10.6, Active Directory

Follow the steps below to force the creation of the Kerberos TGT on initial login.

1. Make a backup copy of the authorization file with this Terminal command:
   ```
   sudo cp /etc/authorization /etc/authorization.bak
   ```
2. Open the /etc/authorization file in a text editor or plist editing application.
3. Locate this key:
   ```
   <key>system.login.console</key>
   ```
4. Under mechanisms, add the string:
   ```
   <string>builtin:krb5store,privileged</string>
   ```
5. Save the file to /etc


Mac OS X Server v10.6: Configuring service principals in Active Directory when using a disjoint namespace
http://support.apple.com/kb/HT3795
Reader
Google
All Products...
Languages
English
日本語
Related Articles
Mac OS X Server v10.6: Configuring iChat Server user attributes wh...
Server Admin 10.6 Help: Configuring Services for Kerberos After Up...
Server Admin 10.6 Help: About Kerberos Principals and Realms
Server Admin 10.6 Help: Using kadmin to Kerberize a Service
Server Admin 10.6 Help: Managing Principals
Related Videos
iPhoto '09: Manage Your Photos Using Events
iMovie '09: Add Video Effects
iPhoto '09: Create and Share a Slideshow
iMovie '09: Adding Background Music to Your Movie
iPhoto '09: Fix Photos That Are Too Dark or Too Light
Related Discussions

Mac OS X Server v10.6: Configuring service principals in Active Directory when using a disjoint namespace

Last Modified: August 27, 2009
Article: HT3795

Summary

If the DNS suffix of the hostname of your Mac OS X Server v10.6-based server does not match the domain name of your Active Directory domain, for example the Active Directory domain is ad.apple.com, but the Mac OS X Server hostname is server.apple.com, services may not be able to use kerberos properly.

Products Affected
Mac OS X Server 10.6 , Microsoft Active Directory

Use ADSI Edit in Active Directory to edit the dNSHostName attribute of the Mac OS X Server computer record to reflect the correct hostname, and the service principals will automatically change.

For example, if your Active Directory domain is:

ad.apple.com

... and the Mac OS X Server hostname is:

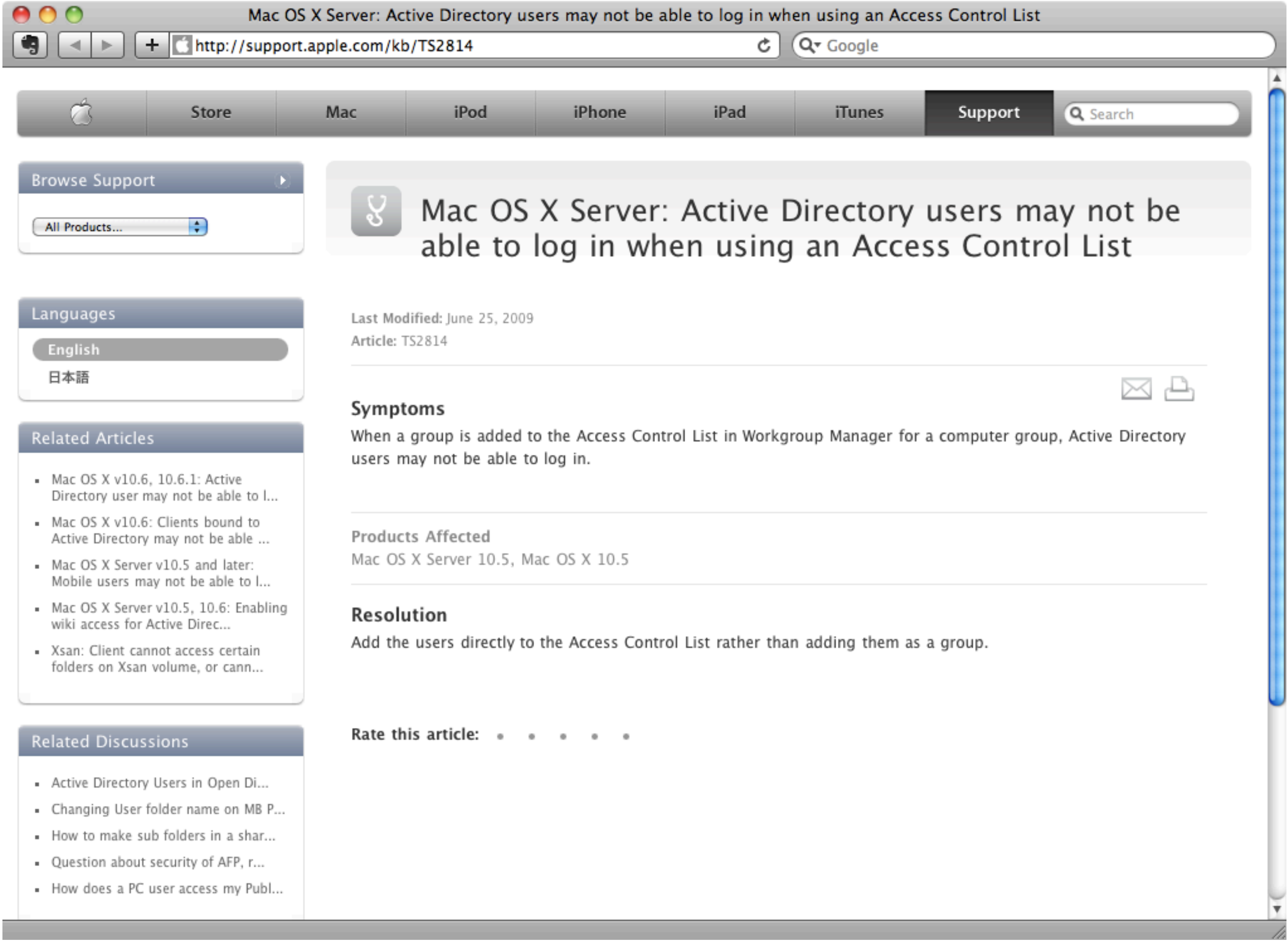
server.apple.com

Edit the dNSHostName attribute of the affected Mac OS X Server computer record from:

server.ad.apple.com

to:

server.apple.com


Mac OS X Server: Active Directory users may not be able to log in when using an Access Control List
http://support.apple.com/kb/TS2814
Google
Store
Mac
iPod
iPhone
iPad
iTunes
Support
Search
Browse Support
All Products...
Languages
English
日本語

Mac OS X Server: Active Directory users may not be able to log in when using an Access Control List

Last Modified: June 25, 2009

Article: TS2814

Symptoms

When a group is added to the Access Control List in Workgroup Manager for a computer group, Active Directory users may not be able to log in.

Products Affected

Mac OS X Server 10.5, Mac OS X 10.5

Resolution

Add the users directly to the Access Control List rather than adding them as a group.

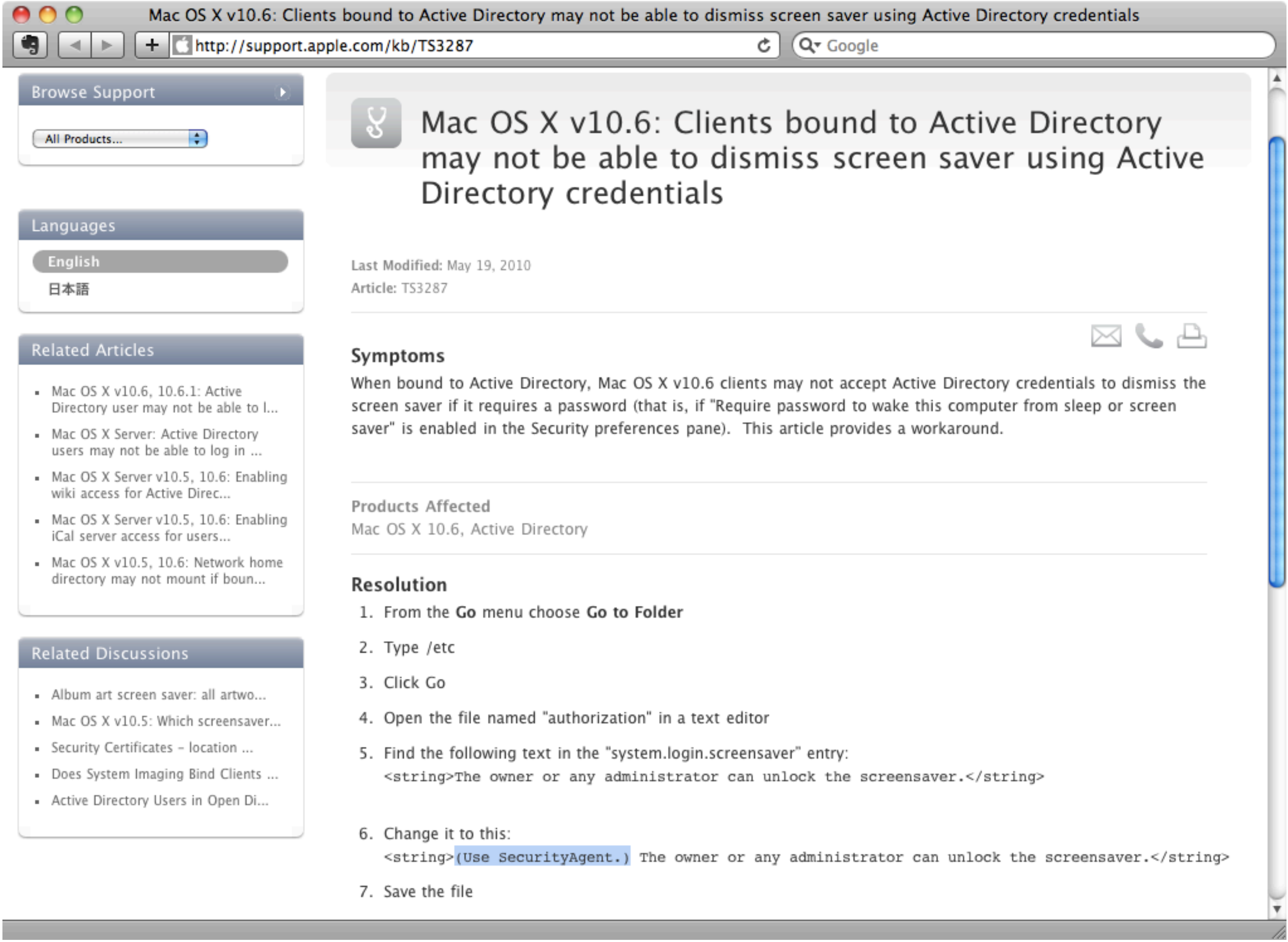
Rate this article: • • • • •

Related Articles

- Mac OS X v10.6, 10.6.1: Active Directory user may not be able to l...
- Mac OS X v10.6: Clients bound to Active Directory may not be able ...
- Mac OS X Server v10.5 and later: Mobile users may not be able to l...
- Mac OS X Server v10.5, 10.6: Enabling wiki access for Active Direc...
- Xsan: Client cannot access certain folders on Xsan volume, or cann...

Related Discussions

- Active Directory Users in Open Di...
- Changing User folder name on MB P...
- How to make sub folders in a shar...
- Question about security of AFP, r...
- How does a PC user access my Publ...


Mac OS X v10.6: Clients bound to Active Directory may not be able to dismiss screen saver using Active Directory credentials
http://support.apple.com/kb/TS3287
Google
Browse Support
All Products...
Languages
English
日本語

Related Articles

- Mac OS X v10.6, 10.6.1: Active Directory user may not be able to l...
- Mac OS X Server: Active Directory users may not be able to log in ...
- Mac OS X Server v10.5, 10.6: Enabling wiki access for Active Direc...
- Mac OS X Server v10.5, 10.6: Enabling iCal server access for users...
- Mac OS X v10.5, 10.6: Network home directory may not mount if boun...

Related Discussions

- Album art screen saver: all artwo...
- Mac OS X v10.5: Which screensaver...
- Security Certificates - location ...
- Does System Imaging Bind Clients ...
- Active Directory Users in Open Di...

Mac OS X v10.6: Clients bound to Active Directory may not be able to dismiss screen saver using Active Directory credentials

Last Modified: May 19, 2010
Article: TS3287

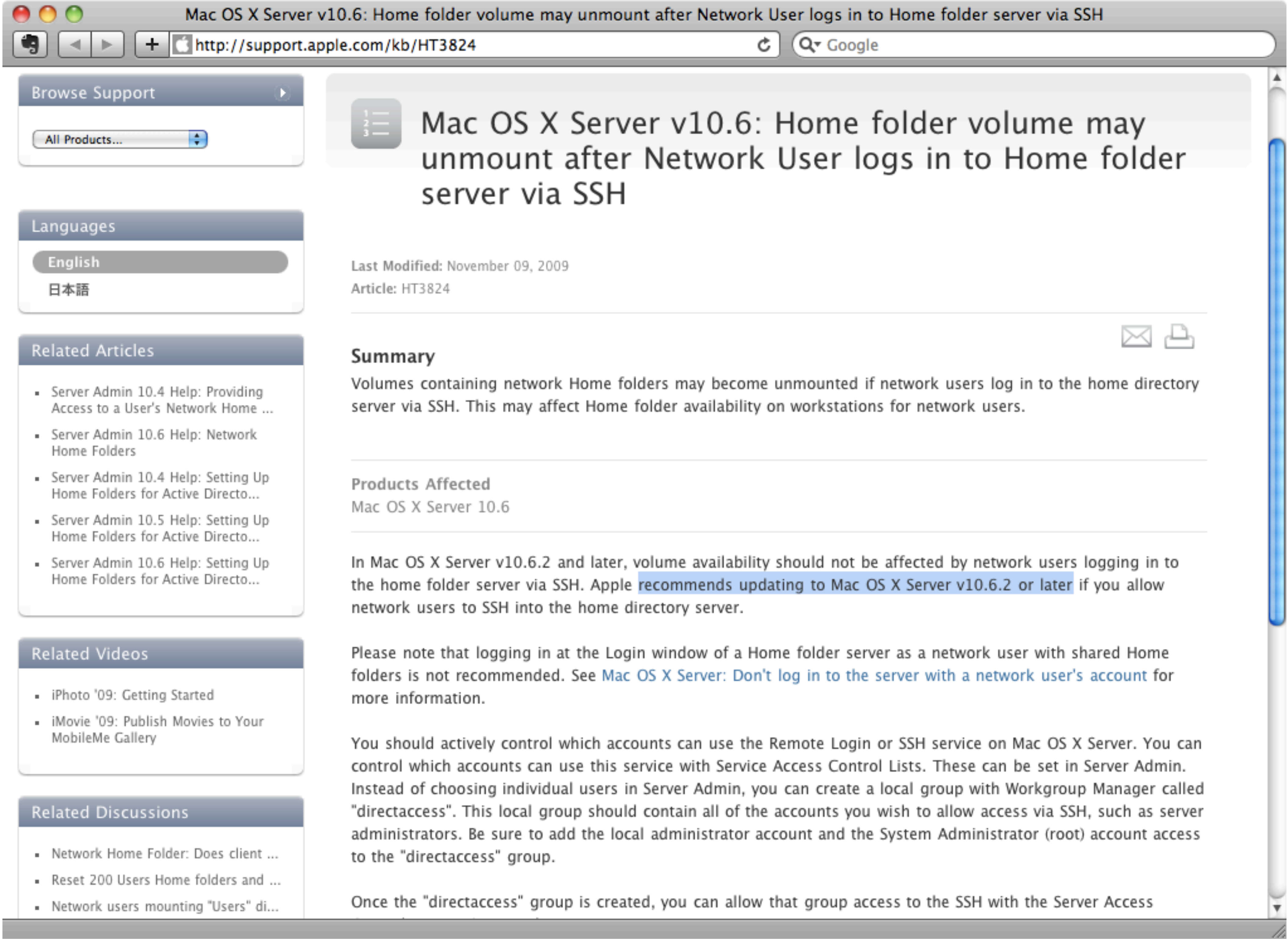
Symptoms

When bound to Active Directory, Mac OS X v10.6 clients may not accept Active Directory credentials to dismiss the screen saver if it requires a password (that is, if "Require password to wake this computer from sleep or screen saver" is enabled in the Security preferences pane). This article provides a workaround.

Products Affected
Mac OS X 10.6, Active Directory

Resolution

1. From the **Go** menu choose **Go to Folder**
2. Type /etc
3. Click Go
4. Open the file named "authorization" in a text editor
5. Find the following text in the "system.login.screensaver" entry:
   ```
   <string>The owner or any administrator can unlock the screensaver.</string>
   ```
6. Change it to this:
   ```
   <string>(Use SecurityAgent.) The owner or any administrator can unlock the screensaver.</string>
   ```
7. Save the file


Mac OS X Server v10.6: Home folder volume may unmount after Network User logs in to Home folder server via SSH
http://support.apple.com/kb/HT3824
Google
Browse Support
All Products...

Languages

- English
- 日本語

Related Articles

- Server Admin 10.4 Help: Providing Access to a User's Network Home ...
- Server Admin 10.6 Help: Network Home Folders
- Server Admin 10.4 Help: Setting Up Home Folders for Active Directo...
- Server Admin 10.5 Help: Setting Up Home Folders for Active Directo...
- Server Admin 10.6 Help: Setting Up Home Folders for Active Directo...

Related Videos

- iPhoto '09: Getting Started
- iMovie '09: Publish Movies to Your MobileMe Gallery

Related Discussions

- Network Home Folder: Does client ...
- Reset 200 Users Home folders and ...
- Network users mounting "Users" di...

Mac OS X Server v10.6: Home folder volume may unmount after Network User logs in to Home folder server via SSH

Last Modified: November 09, 2009

Article: HT3824

Summary

Volumes containing network Home folders may become unmounted if network users log in to the home directory server via SSH. This may affect Home folder availability on workstations for network users.

Products Affected

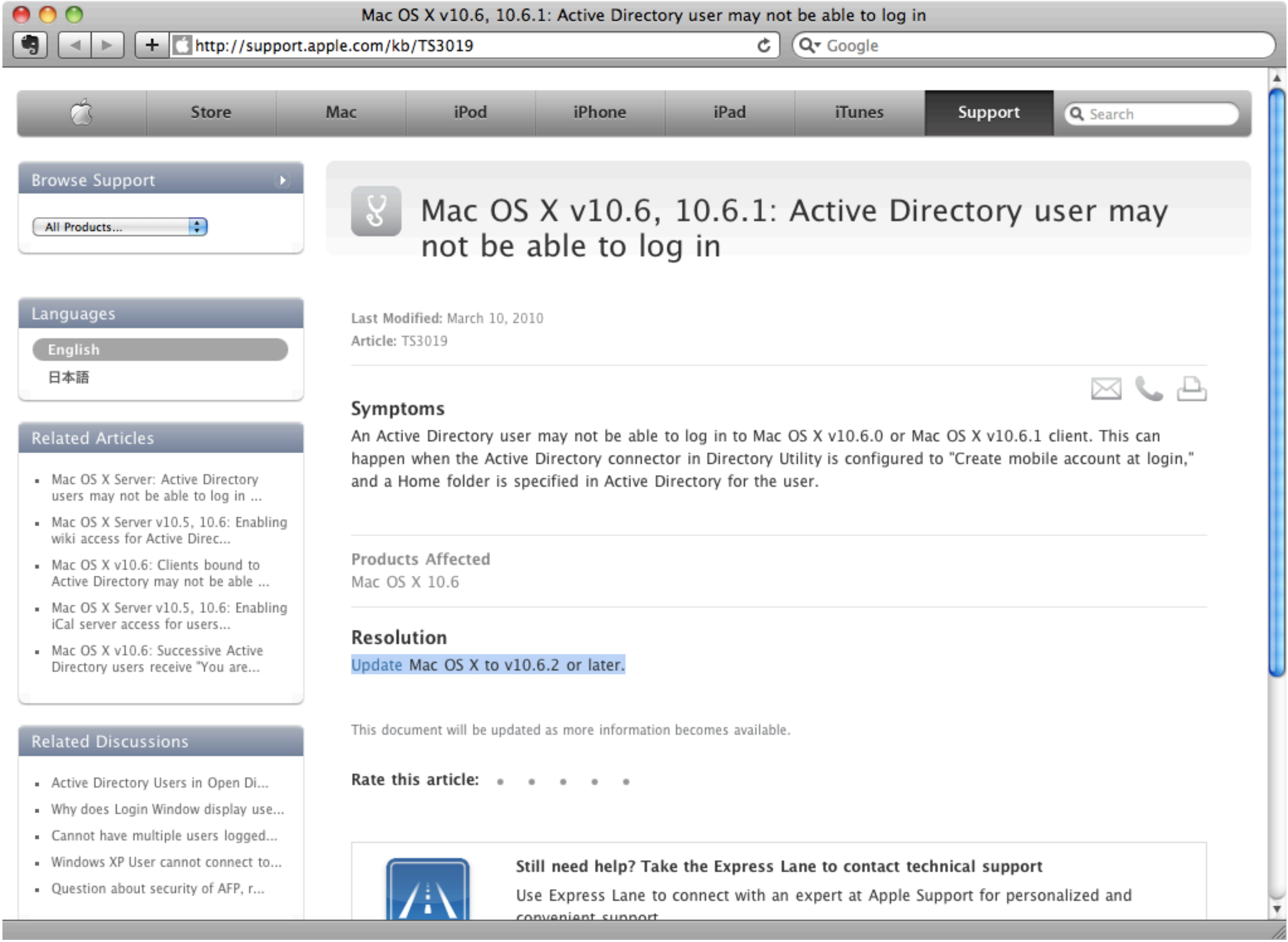
Mac OS X Server 10.6

In Mac OS X Server v10.6.2 and later, volume availability should not be affected by network users logging in to the home folder server via SSH. Apple recommends updating to Mac OS X Server v10.6.2 or later if you allow network users to SSH into the home directory server.

Please note that logging in at the Login window of a Home folder server as a network user with shared Home folders is not recommended. See Mac OS X Server: Don't log in to the server with a network user's account for more information.

You should actively control which accounts can use the Remote Login or SSH service on Mac OS X Server. You can control which accounts can use this service with Service Access Control Lists. These can be set in Server Admin. Instead of choosing individual users in Server Admin, you can create a local group with Workgroup Manager called "directaccess". This local group should contain all of the accounts you wish to allow access via SSH, such as server administrators. Be sure to add the local administrator account and the System Administrator (root) account access to the "directaccess" group.

Once the "directaccess" group is created, you can allow that group access to the SSH with the Server Access


Mac OS X v10.6, 10.6.1: Active Directory user may not be able to log in
http://support.apple.com/kb/TS3019
Google
Store
Mac
iPod
iPhone
iPad
iTunes
Support
Search
Browse Support
All Products...
Languages
English
日本語

Related Articles

- Mac OS X Server: Active Directory users may not be able to log in ...
- Mac OS X Server v10.5, 10.6: Enabling wiki access for Active Direc...
- Mac OS X v10.6: Clients bound to Active Directory may not be able ...
- Mac OS X Server v10.5, 10.6: Enabling iCal server access for users...
- Mac OS X v10.6: Successive Active Directory users receive "You are...

Related Discussions

- Active Directory Users in Open Di...
- Why does Login Window display use...
- Cannot have multiple users logged...
- Windows XP User cannot connect to...
- Question about security of AFP, r...

Mac OS X v10.6, 10.6.1: Active Directory user may not be able to log in

Last Modified: March 10, 2010
Article: TS3019

Symptoms

An Active Directory user may not be able to log in to Mac OS X v10.6.0 or Mac OS X v10.6.1 client. This can happen when the Active Directory connector in Directory Utility is configured to "Create mobile account at login," and a Home folder is specified in Active Directory for the user.

Products Affected

Mac OS X 10.6

Resolution

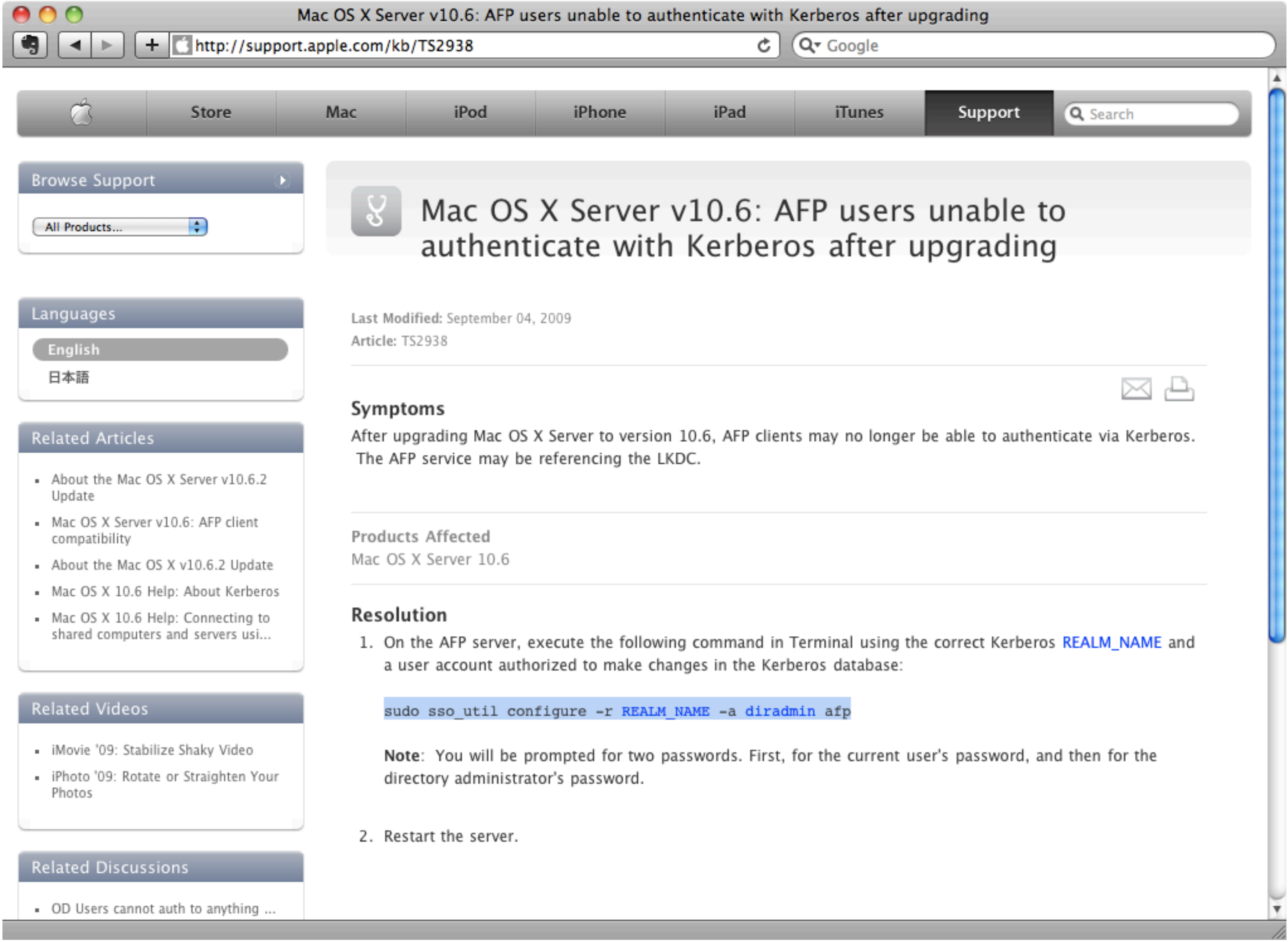
Update Mac OS X to v10.6.2 or later.

This document will be updated as more information becomes available.

Rate this article: ● ● ● ● ●

Still need help? Take the Express Lane to contact technical support

Use Express Lane to connect with an expert at Apple Support for personalized and convenient support


Mac OS X Server v10.6: AFP users unable to authenticate with Kerberos after upgrading
http://support.apple.com/kb/TS2938
Google
Store
Mac
iPod
iPhone
iPad
iTunes
Support
Search
Browse Support
All Products...
Languages
English
日本語
Related Articles
About the Mac OS X Server v10.6.2 Update
Mac OS X Server v10.6: AFP client compatibility
About the Mac OS X v10.6.2 Update
Mac OS X 10.6 Help: About Kerberos
Mac OS X 10.6 Help: Connecting to shared computers and servers usi...
Related Videos
iMovie '09: Stabilize Shaky Video
iPhoto '09: Rotate or Straighten Your Photos
Related Discussions
OD Users cannot auth to anything ...

Mac OS X Server v10.6: AFP users unable to authenticate with Kerberos after upgrading

Last Modified: September 04, 2009

Article: TS2938

Symptoms

After upgrading Mac OS X Server to version 10.6, AFP clients may no longer be able to authenticate via Kerberos. The AFP service may be referencing the LKDC.

Products Affected

Mac OS X Server 10.6

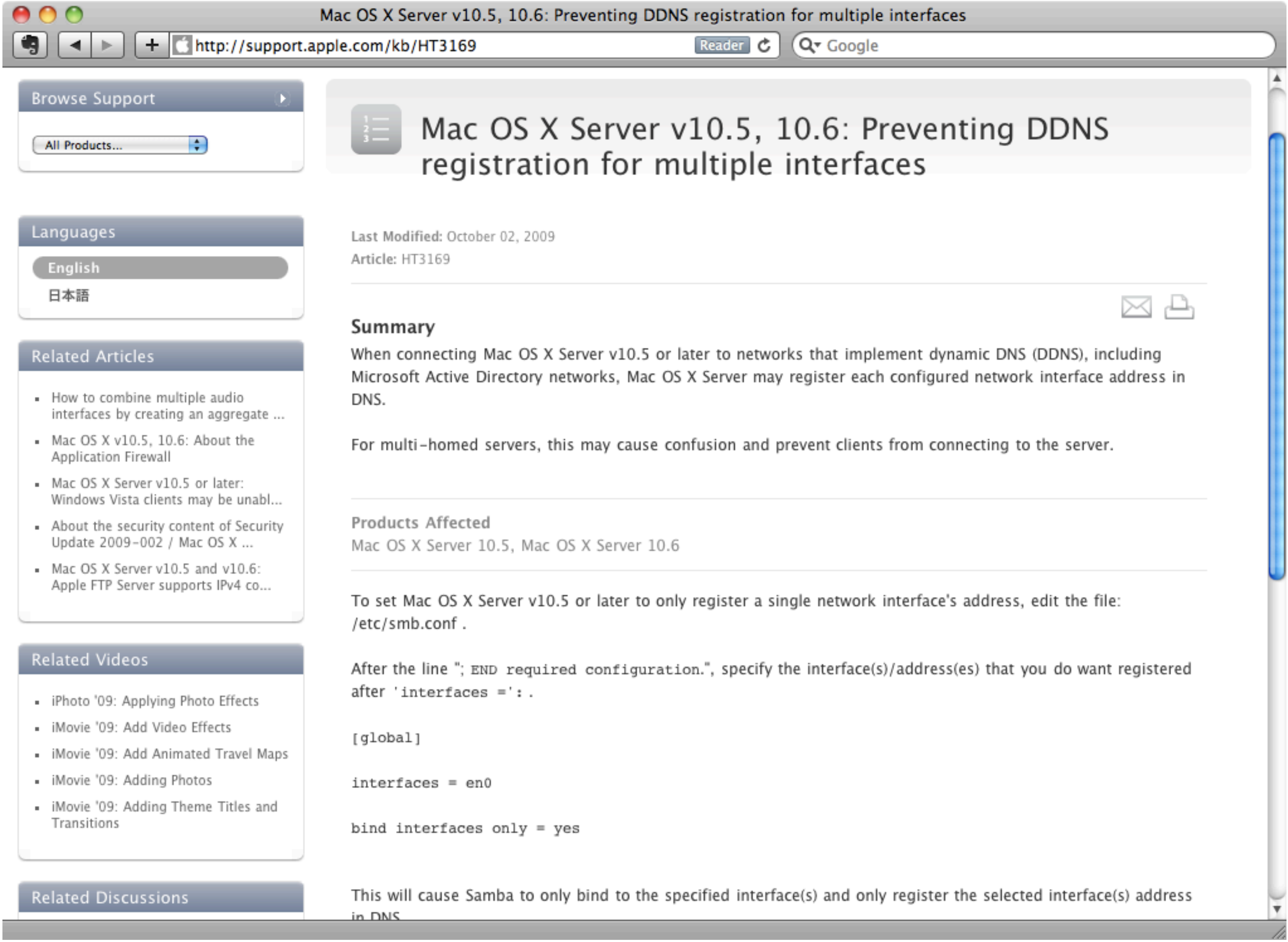
Resolution

1. On the AFP server, execute the following command in Terminal using the correct Kerberos REALM_NAME and a user account authorized to make changes in the Kerberos database:

   ```
   sudo sso_util configure -r REALM_NAME -a diradmin afp
   ```

   Note: You will be prompted for two passwords. First, for the current user's password, and then for the directory administrator's password.

2. Restart the server.


Mac OS X Server v10.5, 10.6: Preventing DDNS registration for multiple interfaces
http://support.apple.com/kb/HT3169
Reader
Google
Browse Support
All Products...
Languages
English
日本語
Related Articles
Related Videos
Related Discussions

- How to combine multiple audio interfaces by creating an aggregate ...
- Mac OS X v10.5, 10.6: About the Application Firewall
- Mac OS X Server v10.5 or later: Windows Vista clients may be unabl...
- About the security content of Security Update 2009-002 / Mac OS X ...
- Mac OS X Server v10.5 and v10.6: Apple FTP Server supports IPv4 co...

- iPhoto '09: Applying Photo Effects
- iMovie '09: Add Video Effects
- iMovie '09: Add Animated Travel Maps
- iMovie '09: Adding Photos
- iMovie '09: Adding Theme Titles and Transitions

Mac OS X Server v10.5, 10.6: Preventing DDNS registration for multiple interfaces

Last Modified: October 02, 2009

Article: HT3169

Summary

When connecting Mac OS X Server v10.5 or later to networks that implement dynamic DNS (DDNS), including Microsoft Active Directory networks, Mac OS X Server may register each configured network interface address in DNS.

For multi-homed servers, this may cause confusion and prevent clients from connecting to the server.

Products Affected

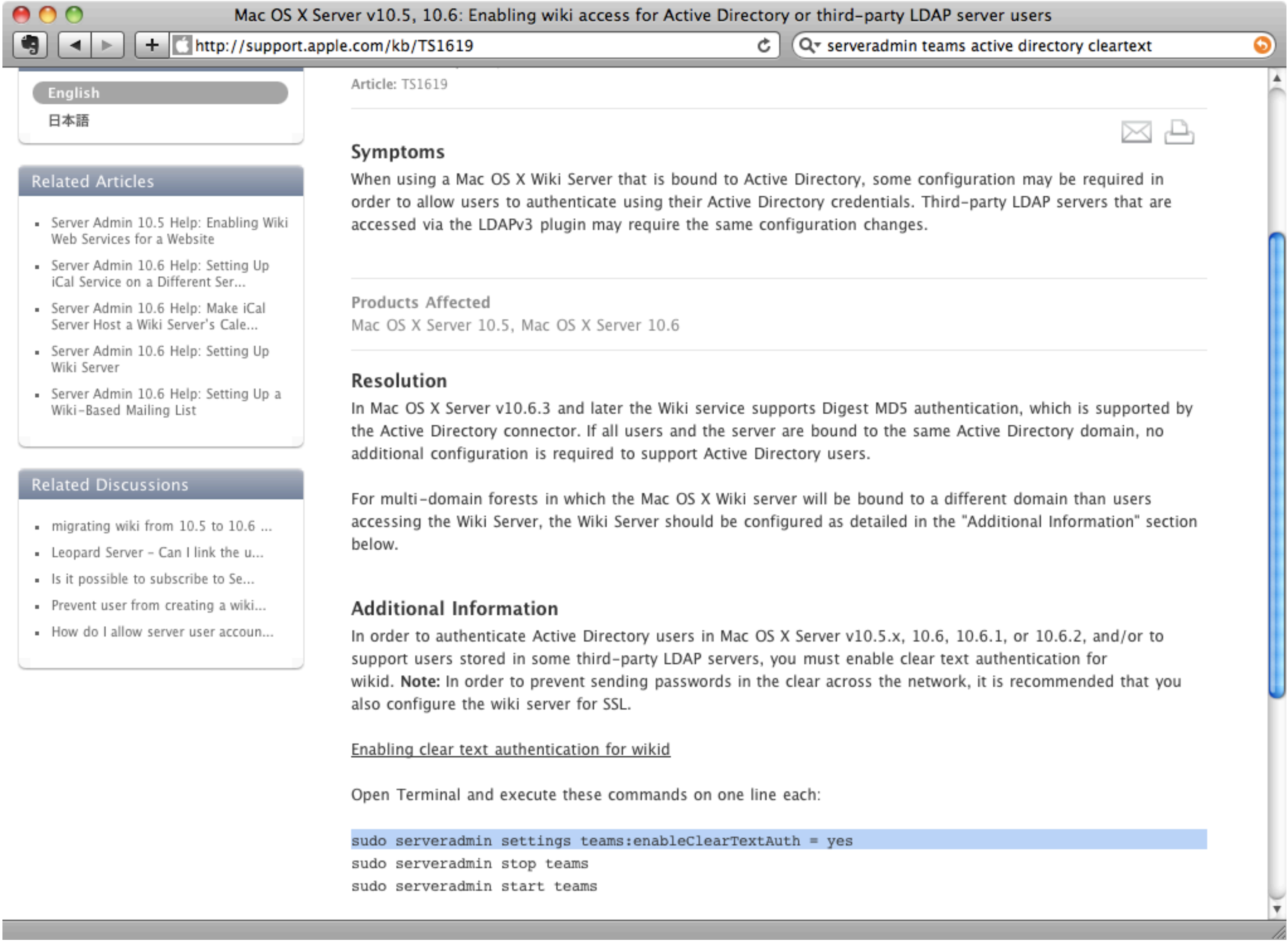
Mac OS X Server 10.5, Mac OS X Server 10.6

To set Mac OS X Server v10.5 or later to only register a single network interface's address, edit the file: /etc/smb.conf .

After the line "; END required configuration.", specify the interface(s)/address(es) that you do want registered after 'interfaces =': .

```
[global]

interfaces = en0

bind interfaces only = yes
```

This will cause Samba to only bind to the specified interface(s) and only register the selected interface(s) address in DNS


Mac OS X Server v10.5, 10.6: Enabling wiki access for Active Directory or third-party LDAP server users
http://support.apple.com/kb/TS1619
serveradmin teams active directory cleartext
English
日本語

Related Articles

- Server Admin 10.5 Help: Enabling Wiki Web Services for a Website
- Server Admin 10.6 Help: Setting Up iCal Service on a Different Ser...
- Server Admin 10.6 Help: Make iCal Server Host a Wiki Server's Cale...
- Server Admin 10.6 Help: Setting Up Wiki Server
- Server Admin 10.6 Help: Setting Up a Wiki-Based Mailing List

Related Discussions

- migrating wiki from 10.5 to 10.6 ...
- Leopard Server - Can I link the u...
- Is it possible to subscribe to Se...
- Prevent user from creating a wiki...
- How do I allow server user accoun...

Article: TS1619

Symptoms

When using a Mac OS X Wiki Server that is bound to Active Directory, some configuration may be required in order to allow users to authenticate using their Active Directory credentials. Third-party LDAP servers that are accessed via the LDAPv3 plugin may require the same configuration changes.

Products Affected
Mac OS X Server 10.5, Mac OS X Server 10.6

Resolution

In Mac OS X Server v10.6.3 and later the Wiki service supports Digest MD5 authentication, which is supported by the Active Directory connector. If all users and the server are bound to the same Active Directory domain, no additional configuration is required to support Active Directory users.

For multi-domain forests in which the Mac OS X Wiki server will be bound to a different domain than users accessing the Wiki Server, the Wiki Server should be configured as detailed in the "Additional Information" section below.

Additional Information

In order to authenticate Active Directory users in Mac OS X Server v10.5.x, 10.6, 10.6.1, or 10.6.2, and/or to support users stored in some third-party LDAP servers, you must enable clear text authentication for wikid. **Note:** In order to prevent sending passwords in the clear across the network, it is recommended that you also configure the wiki server for SSL.

Enabling clear text authentication for wikid

Open Terminal and execute these commands on one line each:

```
sudo serveradmin settings teams:enableClearTextAuth = yes
sudo serveradmin stop teams
sudo serveradmin start teams
```

3 Edge Cases

- Sites concept not used
- Binding account too big
- Computer password problem

Sites not Implemented

- dnsmasq to LIE about DNS
  - only tell client about "close" DCs
  - complete hack

Account too big

- Generic Error
- Packet analysis: Kerberos Request too big

Computer Password

- AD Computer object has a password
- One DC out of sync with the others
- Computer password not the same

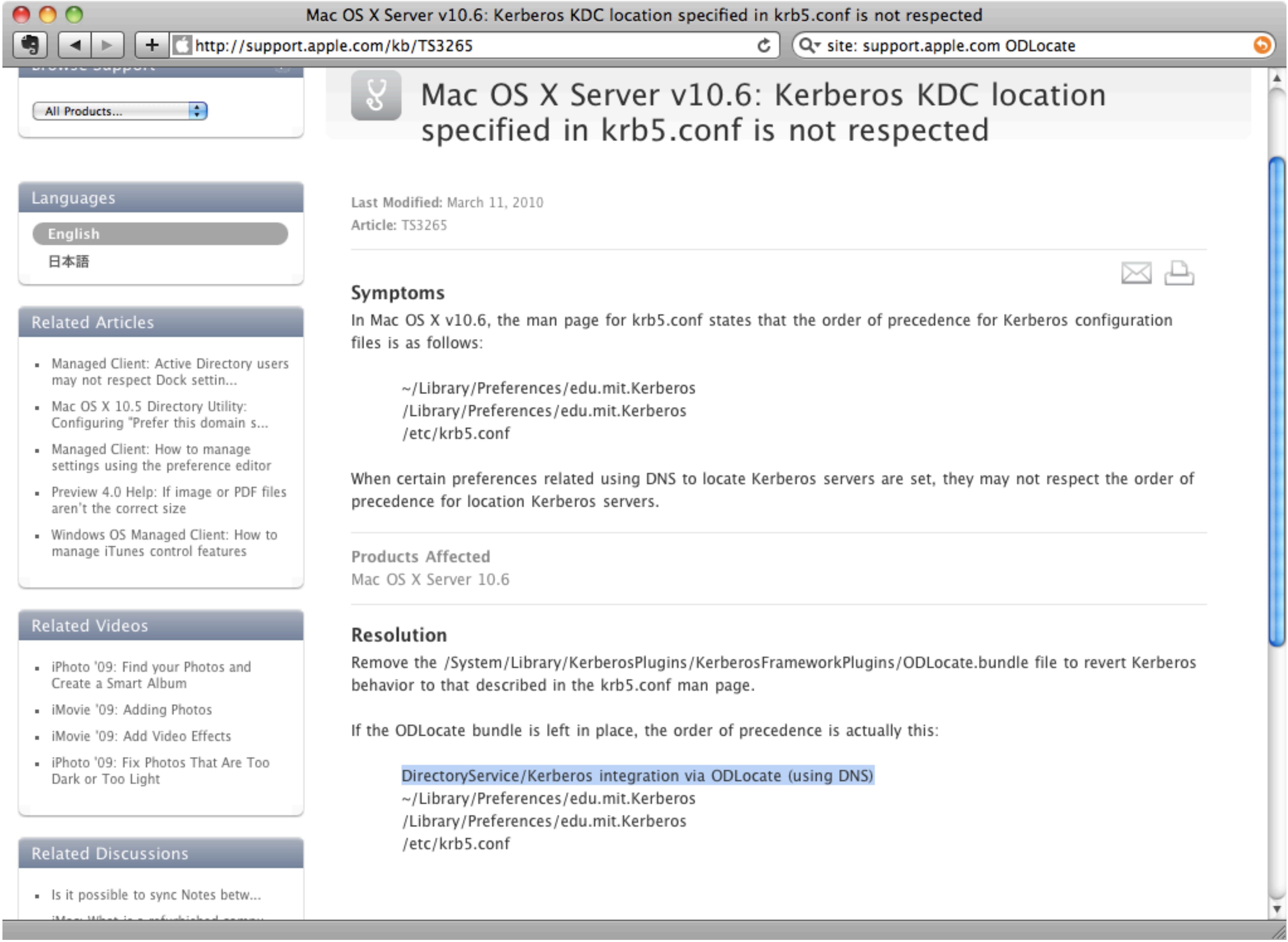
Which dnsRoot

-
  ```
  sudo /usr/libexec/PlistBuddy -c \
  'print dnsRoot' \
  /Library/Preferences\
  /DirectoryService\
  /ActiveDirectoryDomainCache.plist
  ```

Which DC?

-
  ```
  dscl . -read \
  /Config/Kerberos\:SSH22.COM
  ```

```
bash-3.2# dscl
Entering interactive mode... (type "help" for commands)
cd /Local/Default/Config
/Local/Default/Config > cd /Local/Default/Config
/Local/Default/Config > read Kerberos:ADS.EXAMPLE.COM
AppleMetaNodeLocation: /Local/Default
OriginalNodeName:
/Active Directory/All Domains
RecordName: Kerberos:ADS.EXAMPLE.COM
RecordType: dsRecTypeStandard:Config
XMLPlist:
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://
www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
    <key>KADM_List</key>
    <array>
        <string>dc02.ads.example.com.:464</string>
    </array>
    <key>KDC_List</key>
    <array>
        <string>dc02.ads.example.com.:88</string>
    </array>
</dict>
</plist>
```


Mac OS X Server v10.6: Kerberos KDC location specified in krb5.conf is not respected
http://support.apple.com/kb/TS3265
site: support.apple.com ODLocate
All Products...

Languages

English

日本語

Related Articles

- Managed Client: Active Directory users may not respect Dock settin...
- Mac OS X 10.5 Directory Utility: Configuring "Prefer this domain s...
- Managed Client: How to manage settings using the preference editor
- Preview 4.0 Help: If image or PDF files aren't the correct size
- Windows OS Managed Client: How to manage iTunes control features

Related Videos

- iPhoto '09: Find your Photos and Create a Smart Album
- iMovie '09: Adding Photos
- iMovie '09: Add Video Effects
- iPhoto '09: Fix Photos That Are Too Dark or Too Light

Related Discussions

- Is it possible to sync Notes betw...

Mac OS X Server v10.6: Kerberos KDC location specified in krb5.conf is not respected

Last Modified: March 11, 2010

Article: TS3265

Symptoms

In Mac OS X v10.6, the man page for krb5.conf states that the order of precedence for Kerberos configuration files is as follows:

```
~/Library/Preferences/edu.mit.Kerberos
/Library/Preferences/edu.mit.Kerberos
/etc/krb5.conf
```

When certain preferences related using DNS to locate Kerberos servers are set, they may not respect the order of precedence for location Kerberos servers.

Products Affected

Mac OS X Server 10.6

Resolution

Remove the /System/Library/KerberosPlugins/KerberosFrameworkPlugins/ODLocate.bundle file to revert Kerberos behavior to that described in the krb5.conf man page.

If the ODLocate bundle is left in place, the order of precedence is actually this:

```
DirectoryService/Kerberos integration via ODLocate (using DNS)
~/Library/Preferences/edu.mit.Kerberos
/Library/Preferences/edu.mit.Kerberos
/etc/krb5.conf
```

Extract Kerb ID

-
  ```
  #/usr/libexec/PlistBuddy -c \
  'print "AD Computer Kerberos ID"' \
  /Library/Preferences\
  /DirectoryService\
  /ActiveDirectory.plist
  ```
- example: `sever01$@SSH22.COM`

Extract Kerb Pass

-
  ```
  #/usr/libexec/PlistBuddy -c \
  'print "AD Computer Password"' \
  /Library/Preferences\
  /DirectoryService\
  /ActiveDirectory.plist
  ```
- example: `+7gF0oGzdoc70E`

Test password

- `kinit server01$`
- Paste password `(+7gF0oGzdoc70E)`
- `klist`
- `kdestroy`

Don't mask problem

- Unbinding/rebinding only temporary fix

15 Issues Review

- 12 Knowledge Base articles
- 3 Real-world edge cases

What we covered

- Why Integrate
- 3 Challenges
- Terminology Agreement
- 4 Integration Strategies
- 15 Issues unique to AD integration

Thanks

- Questions and Comments
- IM: arekd@me.com
- Email: arek@arekdreyer.com