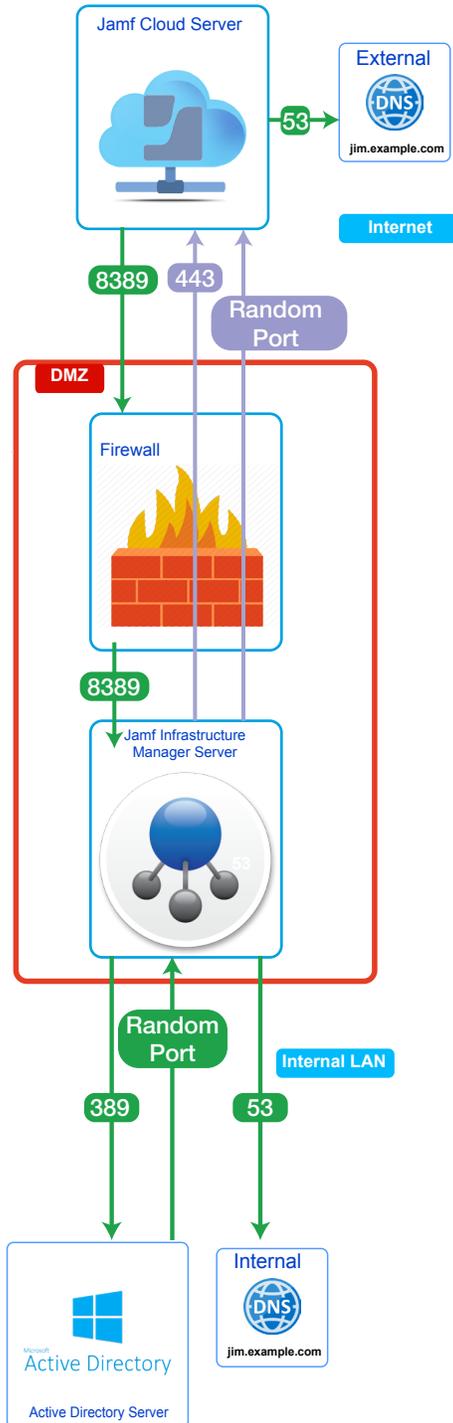




A Guide to
Install Jamf Infrastructure Manager
on a Windows 2016 Server





Internet 1

The Jamf Pro Server needs inbound access to the Jamf Infrastructure Manager Server on port 8389. (If using LDAPS, you can use port 8636).

The Jamf Infrastructure Manager Server makes an outbound connection to the Jamf Cloud Server on port 443.

The Jamf Pro Cloud server will access an External DNS server on port 53. The FQDN must match Externally and Internally on the DNS servers. For example, A DNS record for jim.example.com needs to be on the External and Internal DNS servers.

Firewall-DMZ 2

The Firewall needs to be configured to accept outbound connection requests over port 443 from the Jamf Infrastructure Manager Server and inbound connection requests on port 8389 or 8636 if using LDAPS.

NOTE: Jamf Infrastructure Manager can use any port greater than or equal to 1025. Ports 8389 and 8386 are used in the diagram as an example. The Firewall should accept the requests from the Jamf Cloud Servers in your region listed here:

<https://www.jamf.com/jamf-nation/articles/409/permitting-inbound-outbound-traffic-with-jamfcloud>

When a inbound connection request comes into the Firewall on port 8389 or 8636 if using LDAPS, it will be forwarded to the Jamf Infrastructure Manager Server on port 389 or 636 if using LDAPS. The Firewall should also be configured to allow the Jamf Infrastructure Manager Server access to the Internal DNS server over port 53.

Internal LAN 3

The Jamf Infrastructure Manager Server will send an inbound connection request to the Internal DNS server on port 53 for the FQDN of the Active Directory Server. The Jamf Infrastructure Manager Server will send the initial lookup request to the Active Directory Server on the Internal LAN over port 389 or 636 if using LDAPS.

The Active Directory Server will send its response back to the Jamf Infrastructure Manager Server on a randomly-generated port. The Jamf Infrastructure Manager Server will send the reply back to the Jamf Cloud Server over a randomly-generated port as well.

Acronyms 4

- LDAPS: Lightweight Directory Access Protocol Secure
- AD: Active Directory
- DNS: Domain Name System
- DMZ: Demilitarized Zone
- JIM: Jamf Infrastructure Manager
- LAN: Local Area Network
- FQDN: Fully-Qualified Domain Name

This guide was created using the following:

- Windows Server 2016 Standard Active Directory
- Jamf Infrastructure Manager Version 1.3.1
- Network Address Translation (NAT)

Before you begin:

1. Work with your network team to make sure the following ports are open from the Jamf Infrastructure Manager (JIM) Server:
 - Port 389 for LDAP (or 636 for LDAPS or 3269 for Global Catalog) to an Active Directory Domain Controller.
 - Port 53 to the internal DNS server.
 - Port 443 for outbound traffic to the Jamf Cloud Server (this port is normally open on the firewall).
2. Make sure the following ports are open from the Jamf Cloud Server to the JIM Server:
 - Port 8389 for LDAP (or 8636 for LDAPS).
3. Allow only the Jamf Cloud IP addresses in your region inbound access to the JIM Server. See the IP region list below.

<https://www.jamf.com/jamf-nation/articles/409/permitting-inbound-outbound-traffic-with-jamf-cloud>
4. The fully-qualified domain name of your JIM, for example, infrastructure.example.com, should have a DNS record available on your internal LAN, and a DNS record available to the public. The DNS record inside your LAN should resolve to the internal IPv4 address of your JIM, and the DNS record available to the public should resolve to the public IPv4 address of your JIM.
5. Java JDK 8 is required. Make sure you have it installed on your JIM before starting this guide.



1. Create a user named: jamf-im on the Jamf Pro server and give it custom access.

Account **Privileges**

USERNAME Username for the account
jamf-im

ACCESS LEVEL Level of access to grant the account
Full Access

PRIVILEGE SET Set of privileges to grant the account
Custom

ACCESS STATUS Access status of the account ("enabled" or "disabled")
Enabled

FULL NAME Name of the account holder (e.g. "John Smith")
Jamf Infrastructure Manager

EMAIL ADDRESS Email address for the account (e.g. "john@mycompany.com")

2. Provide Full Access only to the JIM Instances.

Account	Privileges
Jamf Pro Server Objects Create, Read, Update and Delete	Infrastructure Manager Instances

Installing Jamf Infrastructure Manager on Windows 2016 Server

- Using a browser on your JIM server, log in to your Jamf Nation Account and download the latest version of JIM.

Infrastructure Manager

Current Version
Infrastructure Manager 1.3.1

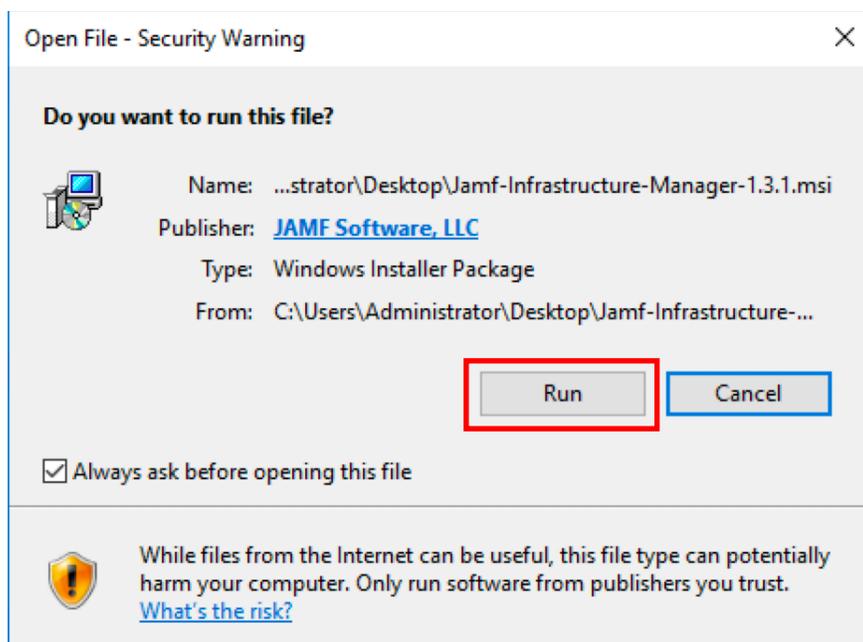
Documentation
[Jamf Infrastructure Manager Installation Guide 1.3.1](#)

 **Download** [MD5 Checksum: 5431530594ab8bb1d1681fd1758b3f64]

- Double Click the JIM 1.3.1 installer.

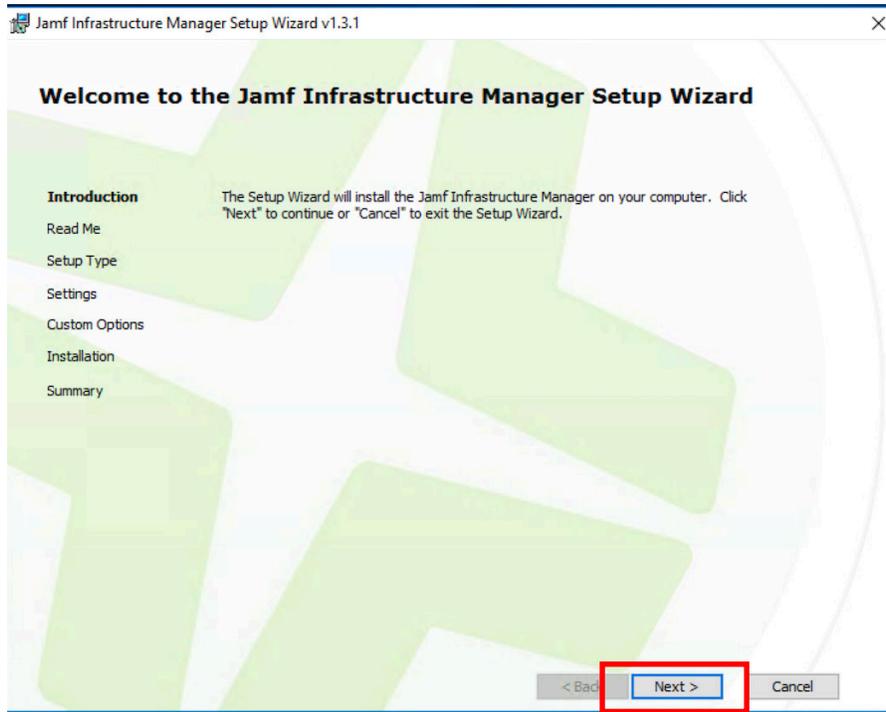


- Click Run.

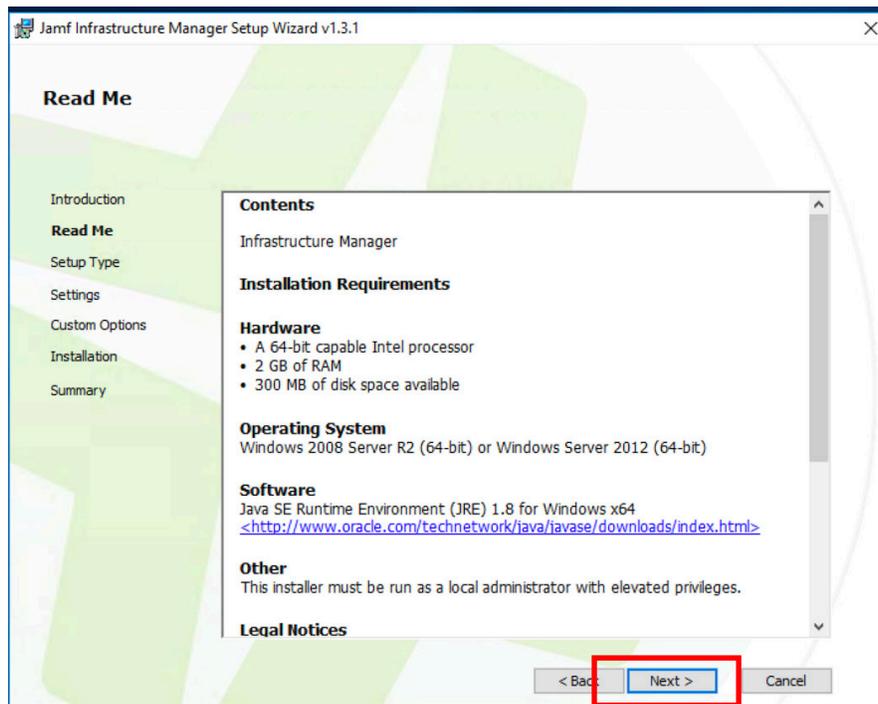




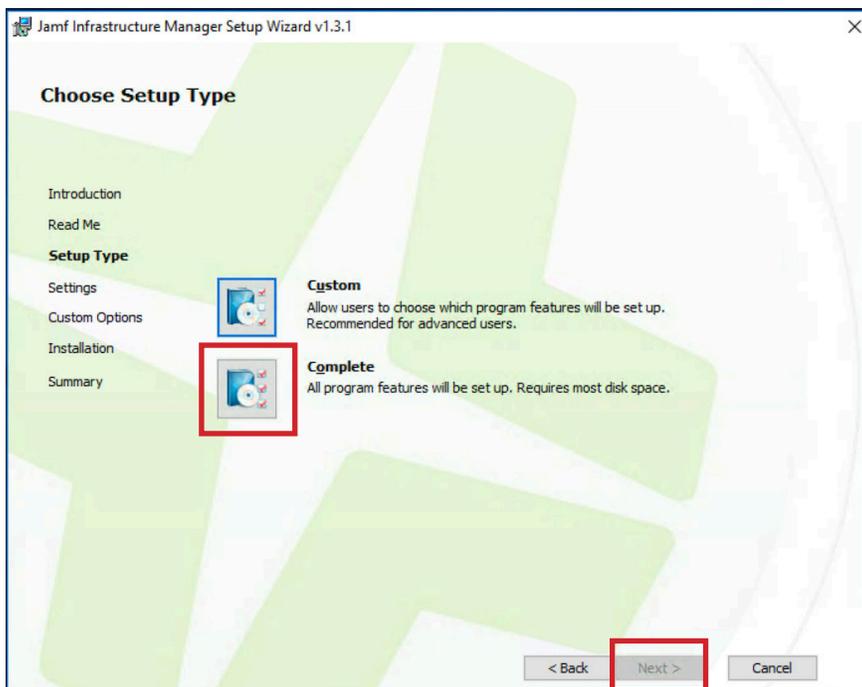
6. Click Next.



7. Click Next.

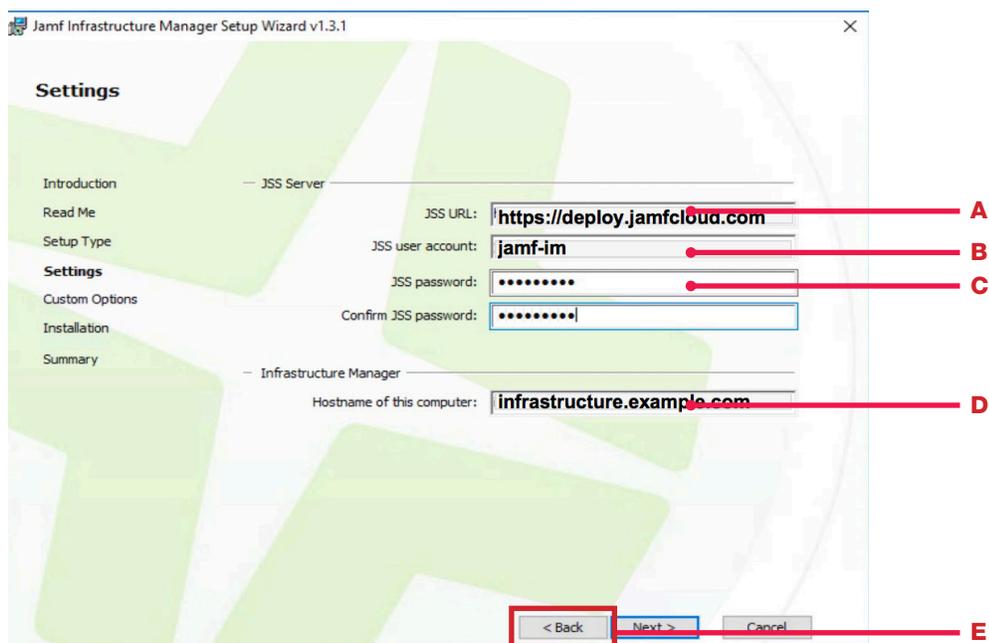


8. Click Complete, then click Next.



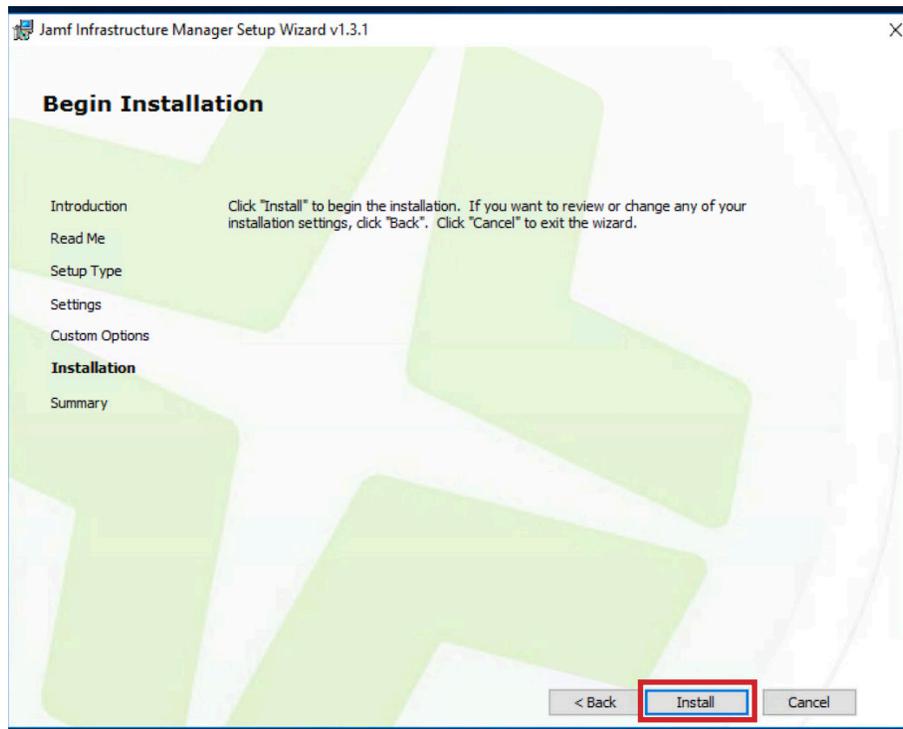
9. Enter the following:

- A. JSS URL: Enter the URL of your Jamf Pro Server.
- B. JSS User Account: jamf-im
- C. Password
- D. Hostname of this computer: Enter the fully-qualified domain name of the computer running JIM.
- E. Click Next.

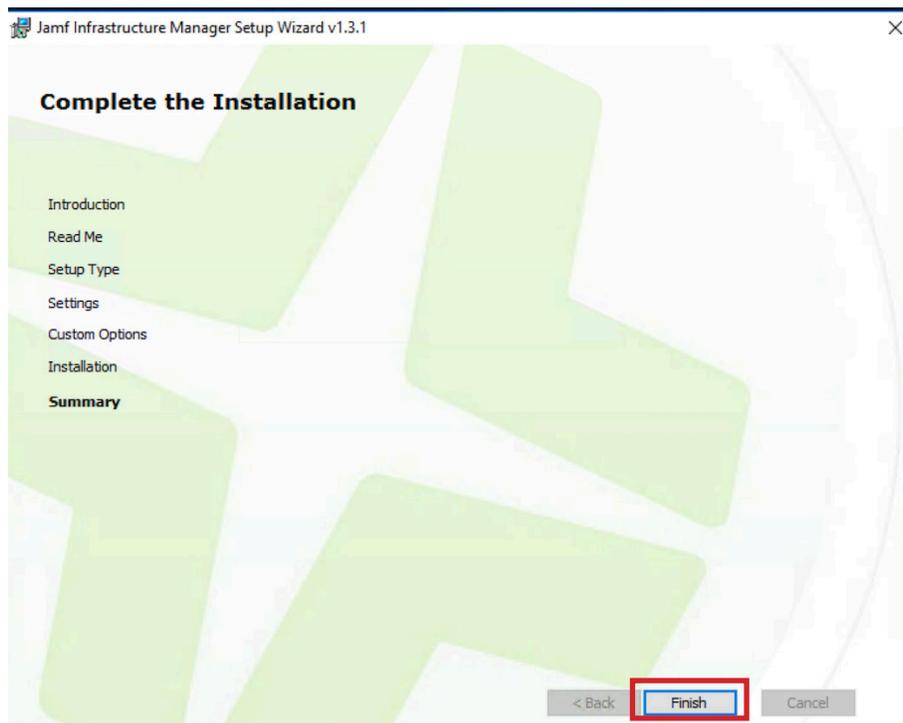




10. Click Install.



11. Click Finish.



12. If your JIM is in the DMZ of your firewall that is using Network Address Translation (NAT), and you do not have an internal DNS server with the FQDN of the internal IPv4 address of your JIM server, you need to create entries for internal IPv4 addresses in the host file of your JIM Server. The file is located in: /Windows/System32/Drivers/etc/hosts

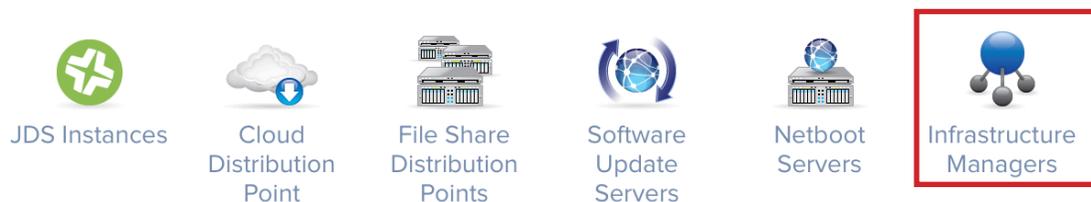
Add the following to the bottom of the file:

- A. The IP address and hostname of your JIM Server in the DMZ.
Example: 192.168.225.4 infrastructure.example.com
- B. The IP address of your Active Directory Server on your LAN. Example:
192.168.100.8 ad.example.com
- C. Save this file when done.

```
Windows.  
#  
# This file contains the mappings of IP addresses to host names.  
Each  
# entry should be kept on an individual line. The IP address  
should  
# be placed in the first column followed by the corresponding  
host name.  
# The IP address and the host name should be separated by at  
least one  
# space.  
#  
# Additionally, comments (such as these) may be inserted on  
individual  
# lines or following the machine name denoted by a '#' symbol.  
#  
# For example:  
#  
#      102.54.94.97      rhino.acme.com      # source server  
#      38.25.63.10      x.acme.com          # x client host  
  
# localhost name resolution is handled within DNS itself.  
#      127.0.0.1        localhost  
#      ::1              localhost  
#      192.168.225.5    infrastructure.example.com  
#      192.168.100.8    ad.example.com
```

13. Log in to your Jamf Pro Server and confirm that the Infrastructure Manager Instance was created and is responding. Select Infrastructure Managers.

Server Infrastructure





14. Make sure the status is Enabled and Last check in succeeded.

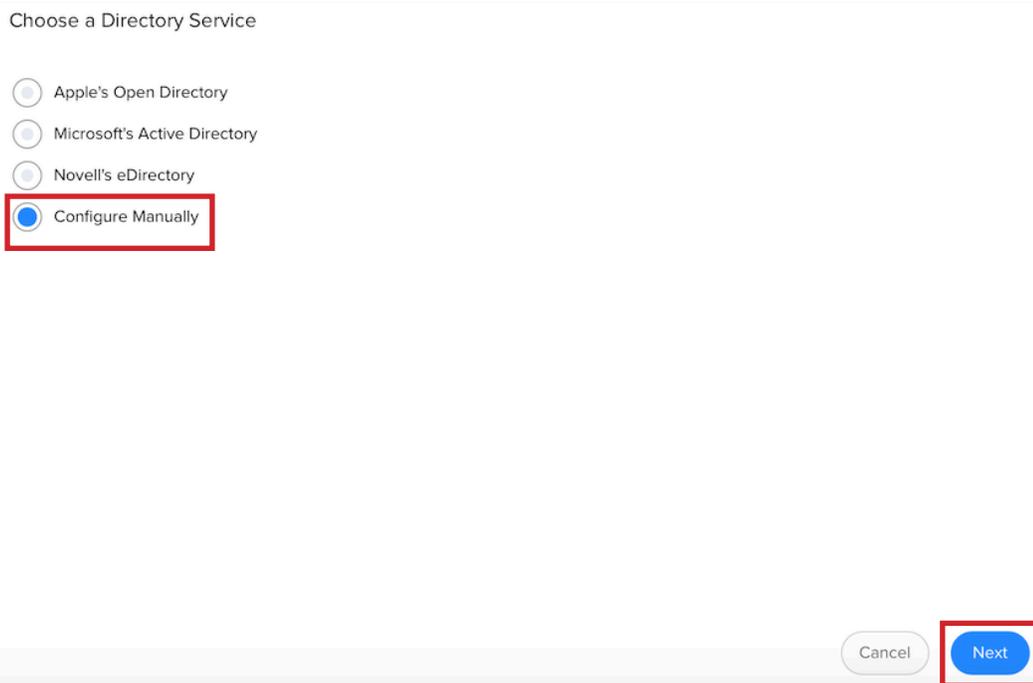
APPLICATION	STATUS	NAME	VERSION	LAST CHECK-IN
LDAP Proxy	Enabled			Less than a minute ago

15. Configure an LDAP server. Go to System Settings, then select LDAP Servers.

System Settings



16. Select Configure Manually, then click Next.



17. Fill out the following:

- A. Display Name: Can be anything you want (this name is not displayed to users).
- B. Server and Port: The hostname of your Active Directory Server and port 389. If connecting to the Global Catalog, use port 3269.
- C. Ensure the checkbox is selected for "Enable LDAP Proxy Server".
- D. Proxy Server: Select your JIM Instance. The port is the port you use to connect to JIM. It can be any port greater than or equal to 1025. This Guide uses 8389 in this example.
- E. Distinguished Name: Enter an account that has access to look up accounts in your Active Directory Server.
- F. Ensure the checkbox is selected for "Use Wildcards When Searching."
- G. Click Mappings in the toolbar.

The screenshot shows the 'Mappings' configuration page in Jamf Infrastructure Manager. The 'Connection' tab is active, and the 'Mappings' sub-tab is selected. The configuration is as follows:

- DISPLAY NAME:** Example JIM
- DIRECTORY SERVICE:** Microsoft's Active Directory
- SERVER AND PORT:** ad.example.com : 389
- ENABLE LDAP PROXY SERVER:** (checked)
- PROXY SERVER:** infrastructure.example.com
- PROXY BINDING ADDRESS AND PORT NUMBER:** infrastructure.example.com : 8389
- USE SSL:** (unchecked)
- AUTHENTICATION TYPE:** Simple
- LDAP SERVER ACCOUNT:** CN=Administrator,CN=Users,DC=example,DC=com
- PASSWORD:** [Redacted]
- VERIFY PASSWORD:** [Redacted]
- CONNECTION TIMEOUT:** 5 Seconds
- SEARCH TIMEOUT:** 60 Seconds
- REFERRAL RESPONSE:** Use default from LDAP service
- USE WILDCARDS WHEN SEARCHING:** (checked)



18. Click "User Mappings."
19. Match your settings to the settings in the screen shot below.
 - A. In the Search Base field, replace the "DC=example,DC=com", with your domain.

User Mappings User Group Mappings

OBJECT CLASS LIMITATION Limitation to set for object classes in the Object Class field
All ObjectClass Values

OBJECT CLASS(ES) Object class(es) to limit results to. Each object class must be separated by a comma
organizationalPerson, user

SEARCH BASE Distinguished name of the search base
A **CN=Users,DC=example,DC=com**

SEARCH SCOPE Hierarchical level to search below the search base
All Subtrees

Attribute Mappings LDAP attribute mappings for Jamf Pro attributes

USER ID
uSNCreated

USERNAME
sAMAccountName

REAL NAME
displayName

EMAIL ADDRESS
userPrincipalName

APPEND TO EMAIL RESULTS Text to append to email address results (e.g. "@mycompany.com")

DEPARTMENT
department

BUILDING
streetAddress

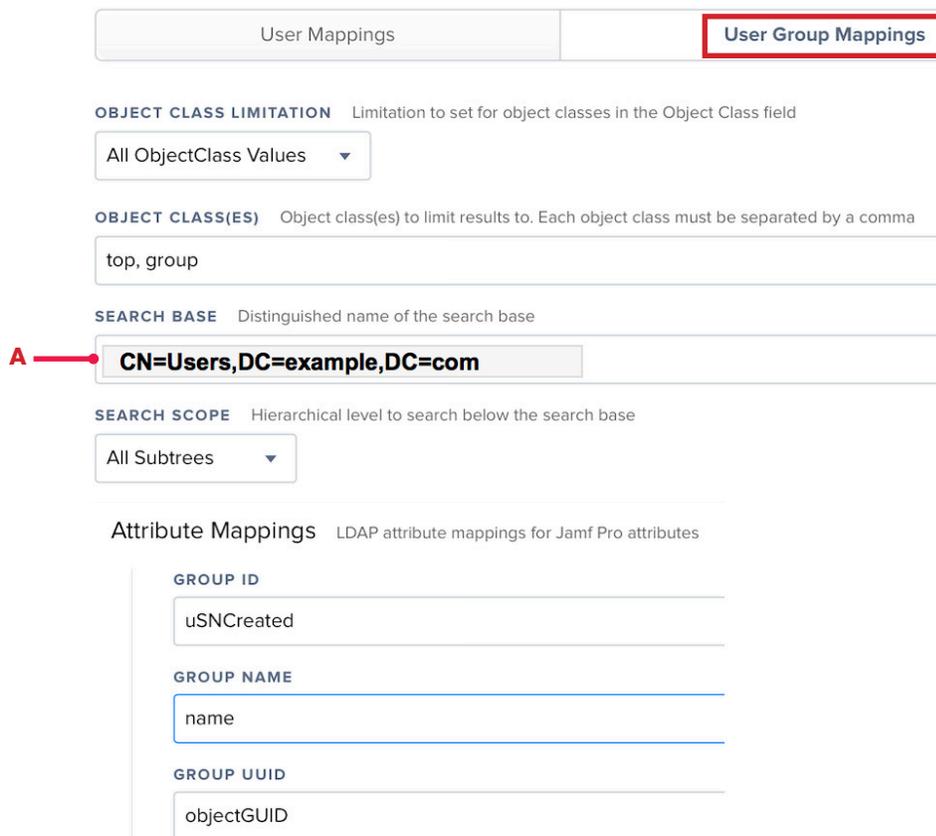
ROOM
streetAddress

PHONE
telephoneNumber

POSITION
title

USER UUID
objectGUID

20. Click “Use Group Mappings.”
21. Match your settings to the settings in the screen shot below.
 - A. In the Search Base field, replace the “DC=example,DC=com”, with your domain.



User Mappings **User Group Mappings**

OBJECT CLASS LIMITATION Limitation to set for object classes in the Object Class field
All ObjectClass Values

OBJECT CLASS(ES) Object class(es) to limit results to. Each object class must be separated by a comma
top, group

SEARCH BASE Distinguished name of the search base
A → CN=Users,DC=example,DC=com

SEARCH SCOPE Hierarchical level to search below the search base
All Subtrees

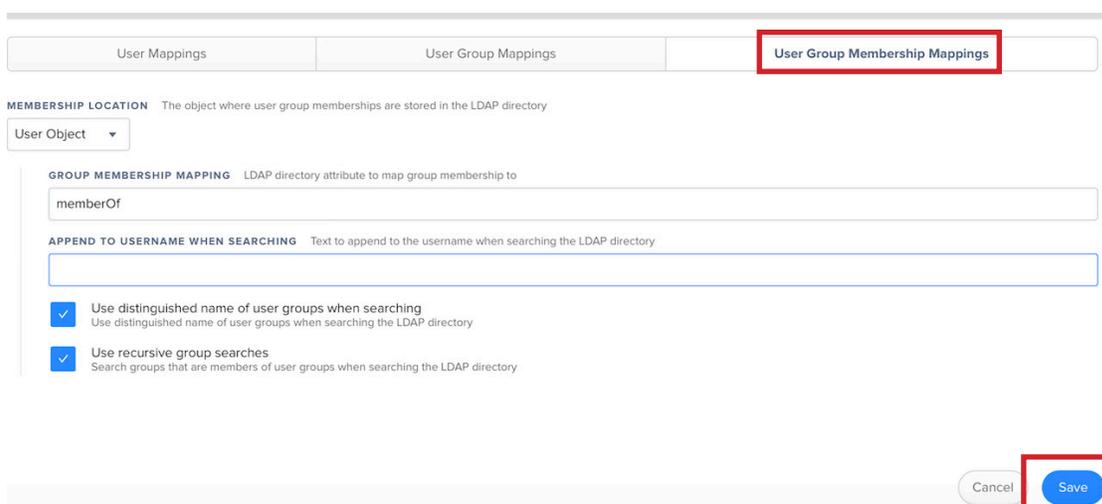
Attribute Mappings LDAP attribute mappings for Jamf Pro attributes

GROUP ID
uSNCreated

GROUP NAME
name

GROUP UUID
objectGUID

22. Click “User Group Membership Mappings.”
23. Match your settings to the settings in the screen shot below. Click Save.



User Mappings User Group Mappings **User Group Membership Mappings**

MEMBERSHIP LOCATION The object where user group memberships are stored in the LDAP directory
User Object

GROUP MEMBERSHIP MAPPING LDAP directory attribute to map group membership to
memberOf

APPEND TO USERNAME WHEN SEARCHING Text to append to the username when searching the LDAP directory

Use distinguished name of user groups when searching
Use distinguished name of user groups when searching the LDAP directory

Use recursive group searches
Search groups that are members of user groups when searching the LDAP directory

Cancel **Save**



- 24. Wait 30 seconds; the JIM connects every 30 seconds to Jamf Pro to check for settings changes.
- 25. Click Test.



- 26. Enter an Active Directory user account name, then click Test.

LOOK UP USERNAME

kmitnick

Test

- 27. If all goes well, you will see the account you just searched for. If all doesn't go well, hit the gym then try again. This completes this guide.

LOOK UP USERNAME

kmitnick

Test

USERNAME	FULL NAME	EMAIL	PHONE	BUILDING	DEPARTMENT	ROOM	POSITION	UID
kmitnick	Keith Mitnick							15771

0.39 seconds