

# Authentication of Ezeelogin gateway users using Public keys fetched from Active Directory server

407 Riya Francis July 31, 2024 [Features & Functionalities](#), [Technical](#) 5275

## Authentication of SSH users using Public keys fetched from the Active Directory server

---

**Overview:** This article describes the process for extending the Active Directory schema to add SSH key attributes on Windows Server 2012 and 2016, including schema updates, attribute and class creation, user association, and integrating with Ezeelogin for SSH key retrieval.

---

- Extending the Active Directory schema to add SSH key attributes in Windows Server 2012 and 2016.

1. **Launch a cmd prompt** then spin up an Administrator cmd by running the following script.

```
C:\Users\Administrator> runas /user:DOMAINAdministrator cmd
```

- You'll get the following terminal after running the above command on cmd.

CA. Command Prompt

```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\Riya>runas /user:EZELOGIN\Administrator cmd
Enter the password for EZELOGIN\Administrator:
Attempting to start cmd as user "EZELOGIN\Administrator" ...

C:\Users\Riya>
```

CA. Administrator: cmd (running as EZELOGIN\Administrator)

```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Windows\system32>
```

2. To open the Registry Editor run the following command on Administrator cmd.

```
C:\Windows\system32> regedit
```

3. Enabling Schema updates in Registry Editor

Browse to **HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Parameters** and add a new DWORD key named **Schema Update Allowed**.

Registry Editor

File Edit View Favorites Help

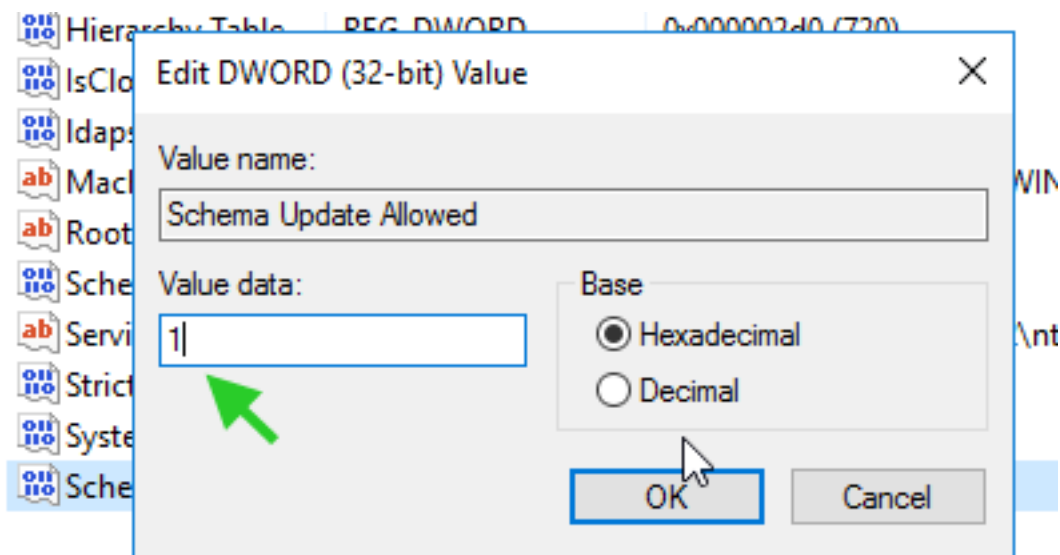
Left pane (Tree view):

- npsvctrig
- nsi
- nsiproxy
- NTDS
  - Diagnostics
  - Parameters
  - Performance
  - RID Values
  - Security
- NtFrs
- NTFS
- Null
- nvraid
- nvstor
- OneSyncSvc
- OneSyncSvc\_ff869
- Parport
- partmgr
- PcaSvc
- pci
- pciide
- pcmcia
- pcw
- pdc
- PEAUTH

Right pane (List view):

Name	Type	Data
(Default)	REG_SZ	(value not set)
Configuration NC	REG_SZ	CN=Configuration,DC=Ezeelogin,DC=com
Database backu...	REG_SZ	C:\Windows\NTDS\dsadata.bak
Database log fil...	REG_SZ	C:\Windows\NTDS
Database loggin...	REG_SZ	ON
DS Drive Mappi...	REG_MULTI_SZ	c:\?\Volume{e2cd9ffb-0000-0000-0000-501f000...
DSA Database E...	REG_DWORD	0x00001922 (6434)
DSA Database file	REG_SZ	C:\Windows\NTDS\ntds.dit
DSA Working Di...	REG_SZ	C:\Windows\NTDS
DsaOptions	REG_SZ	1
Global Catalog ...	REG_DWORD	0x00000001 (1)
Hierarchy Table ...	REG_DWORD	0x000002d0 (720)
IsClone	REG_DWORD	0x00000000 (0)
Idapserverintegr...	REG_DWORD	0x00000001 (1)
Machine DN Na...	REG_SZ	CN=NTDS Settings,CN=WIN-KC4AJFLCLGR,CN=S...
Root Domain	REG_SZ	DC=Ezeelogin,DC=com
Schema Version	REG_DWORD	0x00000057 (87)
ServiceDll	REG_EXPAND_SZ	%systemroot%\system32\ntds.dll
Strict Replicatio...	REG_DWORD	0x00000001 (1)
System Schema...	REG_DWORD	0x00000057 (87)

- Add Dword with value name Schema Update Allowed and value data 1.



4. Run the following in the Administrator command prompt to enable the schema editor snap-in.

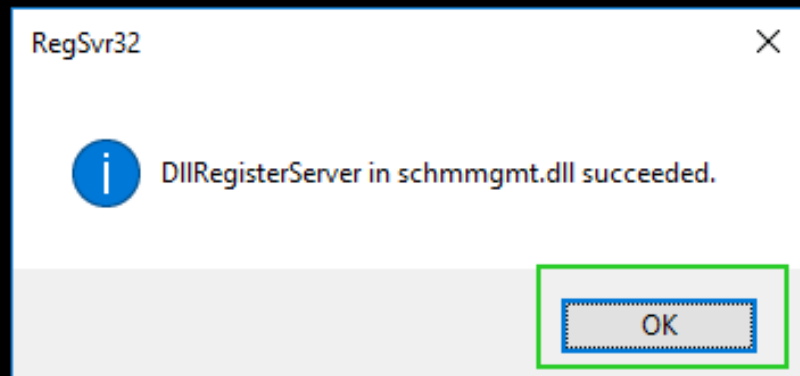
```
c:\Windowssystem32> regsvr32 schmmgmt.dll
```

C:\> Administrator: cmd (running as EZEELGIN\Administrator)

```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

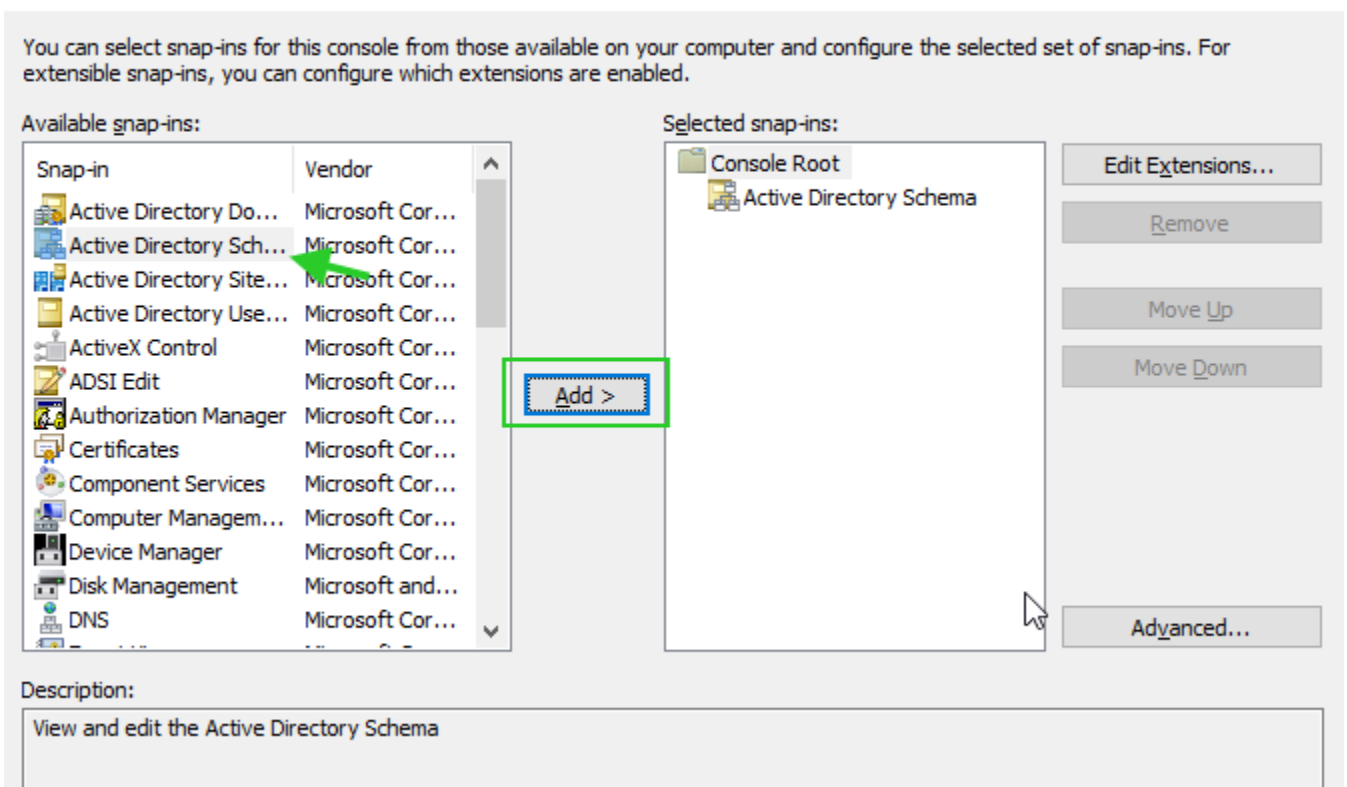
C:\Windows\system32>regsvr32 schmmgmt.dll

C:\Windows\system32>
```



5. Run **mmc** in the Administrator command prompt to open the Management console. Click on Ctrl + M and add Active Directory Schema as follows.

## Add or Remove Snap-ins



### 6. Creating a new attribute in Active Directory.

Right Click on Attributes and click 'Create New Attribute'. Provide the Common Name and LDAP Display Name as **sshPublicKeys**, 'Unique X500 Object ID' as **1.3.6.1.4.1.24552.1.13**, Syntax, select **IA5-String**, finally select the **Mutli-Valued** box, and click **Okay**.

Create New Attribute

Create a New Attribute Object

Identification

Common Name: sshPublicKeys

LDAP Display Name: sshPublicKeys

Unique X500 Object ID: 1.3.6.1.4.1.24552.1.1.1.13

Description:

Syntax and Range

Syntax: IA5-String

Minimum:

Maximum:

☒ Multi-Valued

OK Cancel Help

7. Create a new class for the attribute.

Right-click on Classes and click 'Create class'. Add 'Common Name' and 'LDAP Display Name', as **ldapPublicKey**, 'Unique X500 Object ID' as **1.3.6.1.4.1.24552.500.1.1.2.0**, Parent Class as **'top'**, and for Class Type select **'Auxiliary'**. After providing the necessary fields click on the **Next** button.


## Create New Schema Class



### Identification


Common Name:  ldapPublicKey


LDAP Display Name: ldapPublicKey

Unique X500 Object ID:  1.3.6.1.4.1.24552.500.1.1.2.0

Description:

### Inheritance and Type

Parent Class:  top

Class Type:  Auxiliary

< Back

Next >

Cancel

Help

- Add **sshPublicKey**s under Optional as follows.



## Create New Schema Class



Mandatory:

Add...

Remove

Optional:

sshPublicKeys

Add...

Remove

< Back

Finish

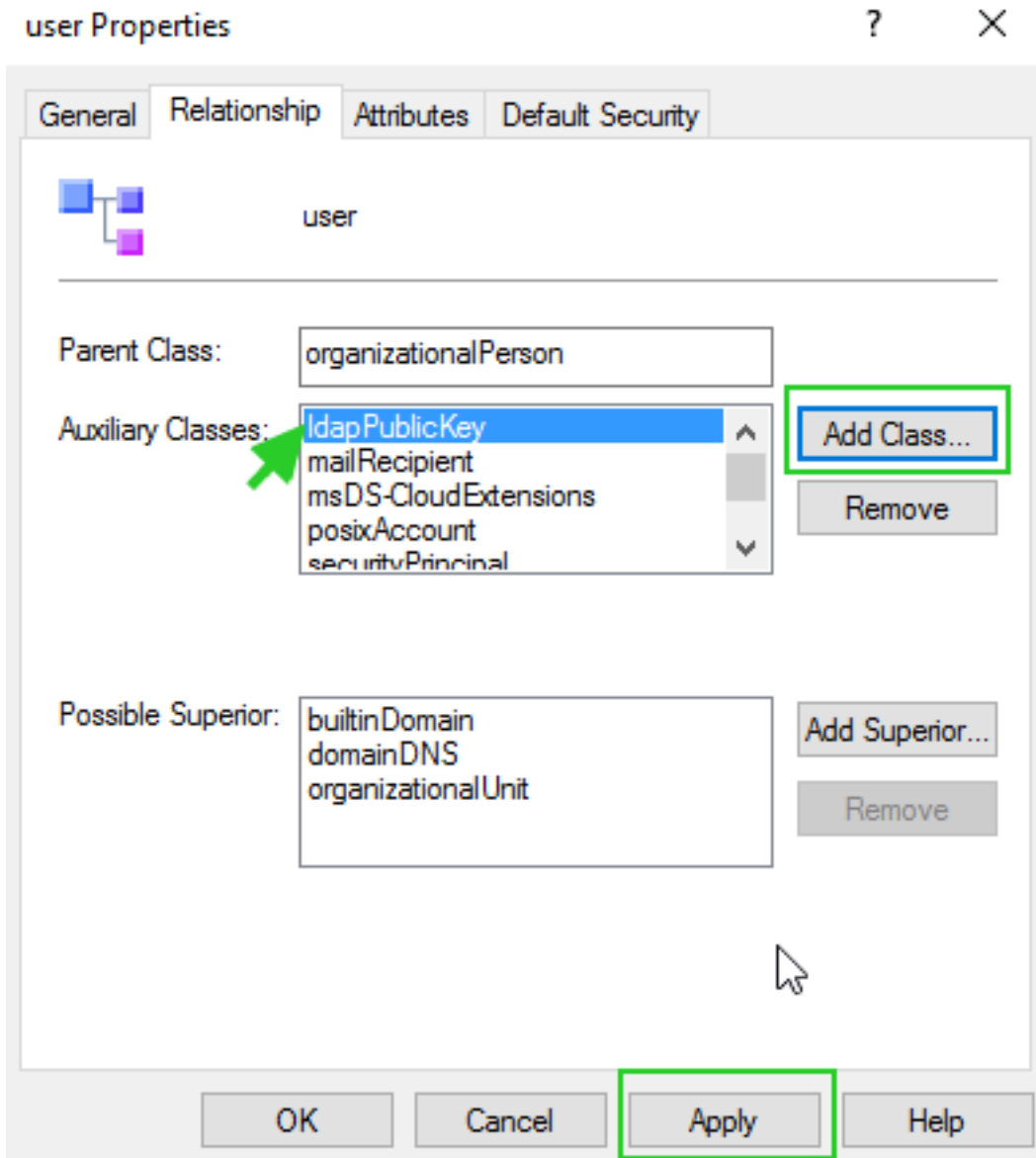
Cancel

Help

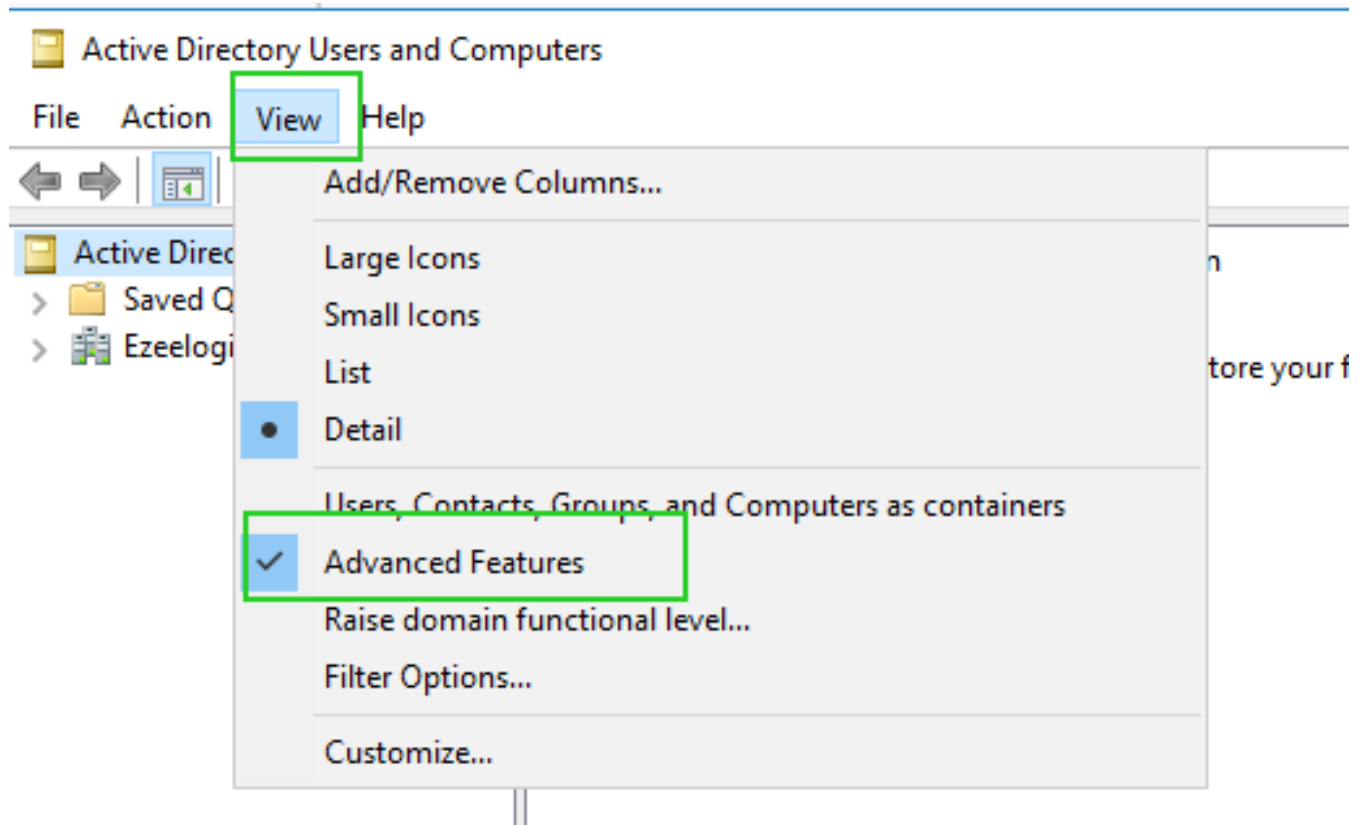
### 8. Associating that class to user objects.

Expand the Classes and right-click on **User** then select **properties**. Click on the **Relationship** tab then click **Add Class** under **Auxiliary class**.

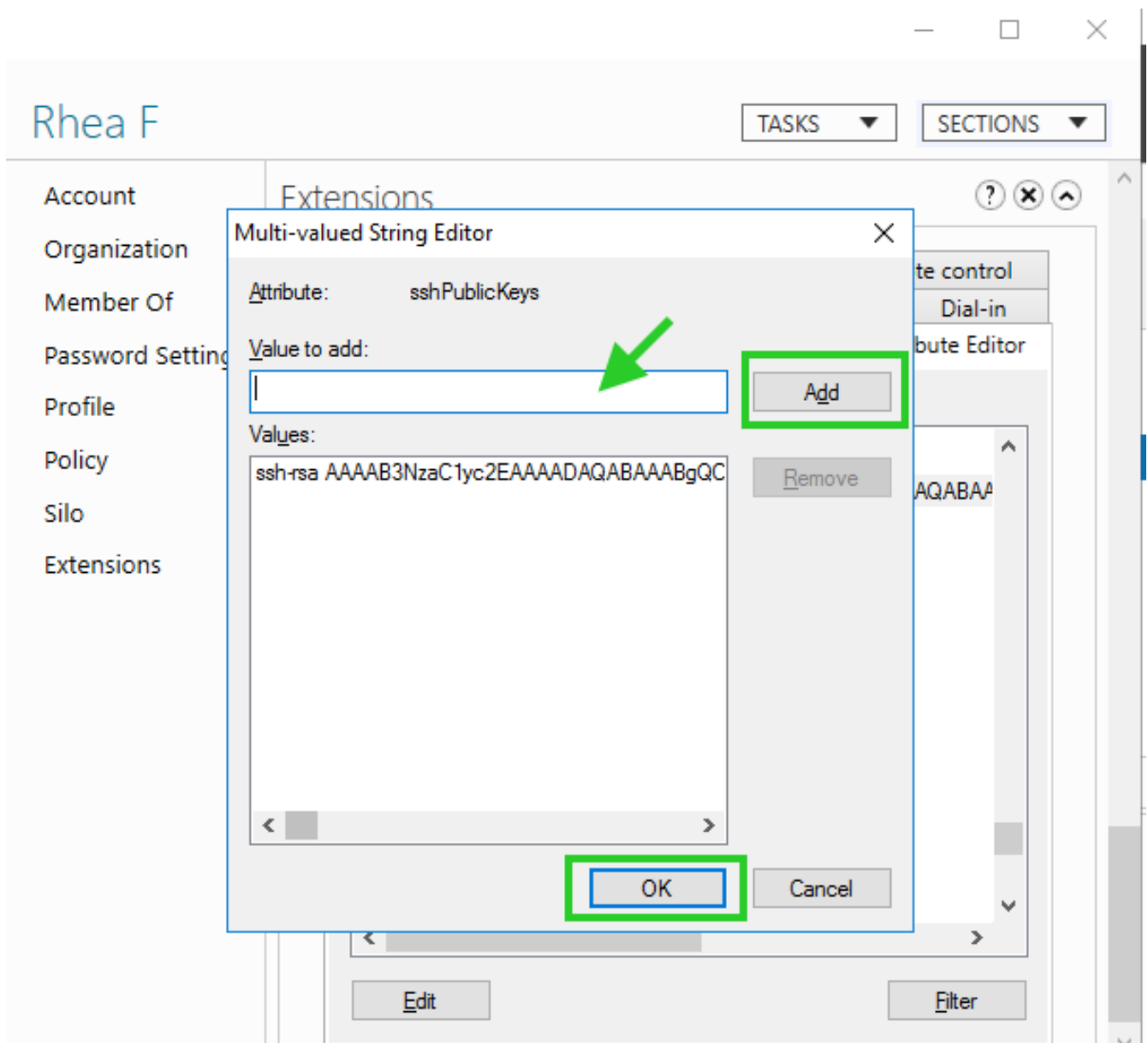
Finally, Add **ldapPublicKey** and click 'Apply'.



9. Close all other windows open Active Directory Users and Computers(ADUC) and enable the **Advanced feature** as follows.



10. Browse to the user and add public keys under **Extensions >> Attribute Editor >> sshPublicKeys**.



## 11. Creating script on Ezeelogin server to fetch SSH key from AD

- Create the following script on your Ezeelogin server under /usr/local/fetchsshkeys.

**Note:** Replace the Basedn, Hostname\_or\_IP , Binddn , and Password with your Active Directory credentials.

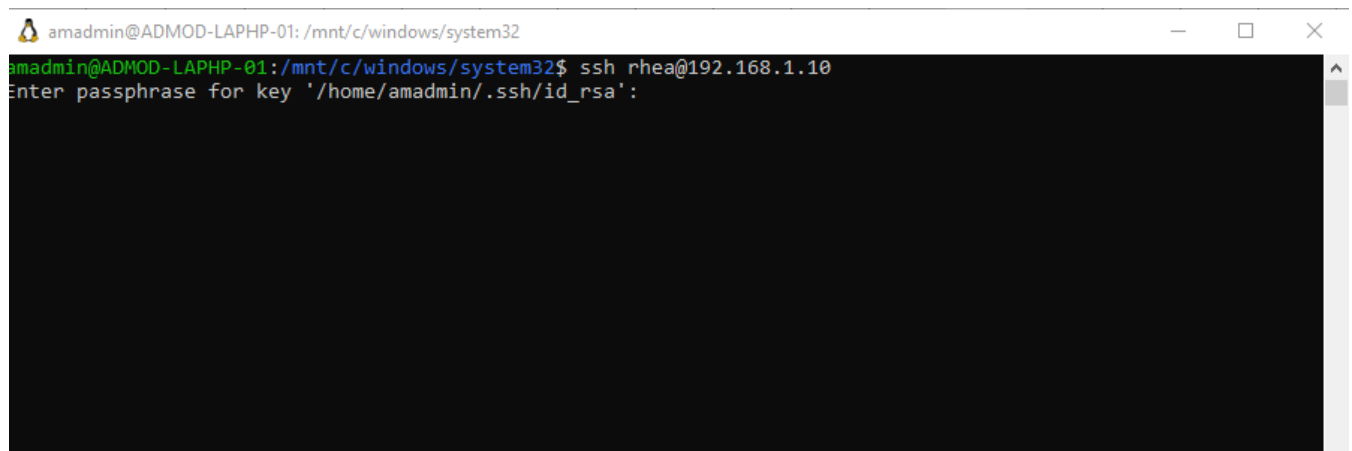
```
#!/bin/bash
```

```
ldapsearch -x '(&(objectClass=*)(sAMAccountName="$1"))' 'sshPublicKeys' -b "Base DN" -H  
ldap://Hostname_or_IP -D "Bind_RDN" -w 'password' | sed -n '/^  
/{H;d};/sshPublicKeys:/x;$g;s/n */g;s/sshPublicKeys: //gp'
```

12. Add the following lines on the gateway server to your `sshd_config` file to point to the script

```
AuthorizedKeysCommand /usr/local/fetchsshkeys  
  
AuthorizedKeysCommandUser root
```

- Now, the user "rhea" will be authenticated using the public key fetched from the Active Directory server.



```
amadmin@ADMOD-LAPHP-01: /mnt/c/windows/system32  
amadmin@ADMOD-LAPHP-01:/mnt/c/windows/system32$ ssh rhea@192.168.1.10  
Enter passphrase for key '/home/amadmin/.ssh/id_rsa':
```

### Troubleshooting steps:

**1. Ensure that the ssh public key is fetched for the user rhea from the Openldap server by running the following command:**

```
root@jumpserver:~# ldapsearch -x '(&(objectClass=*)(sAMAccountName="rhea"))' 'sshPublicKeys'  
-b "OU=EzAdmin,DC=Ezeelogin,DC=com" -H ldap://192.168.1.7 -D  
"cn=Administrator,cn=Users,dc=Ezeelogin,dc=com" -w 'zaQ!23edc123' | sed -n '/^  
/{H;d};/sshPublicKeys:/x;$g;s/n */g;s/sshPublicKeys: //gp'
```

**2. Ensure that the ssh public key is fetched for the user rhea from Ezeelogin installed server by**

### running the script:

```
root@jumpserver:~# /usr/local/fetchsshkeys rhea
```

---

### **Related Articles:**

[Install and set up an active Directory.](#)

[Integrate SAML Authentication with Ezeelogin.](#)

Online URL:

<https://www.ezeelogin.com/kb/article/authentication-of-ezeelogin-gateway-users-using-public-keys-fetched-from-active-directory-server-407.html>