Contents

1. Adding und Testing the Customize AD Schema

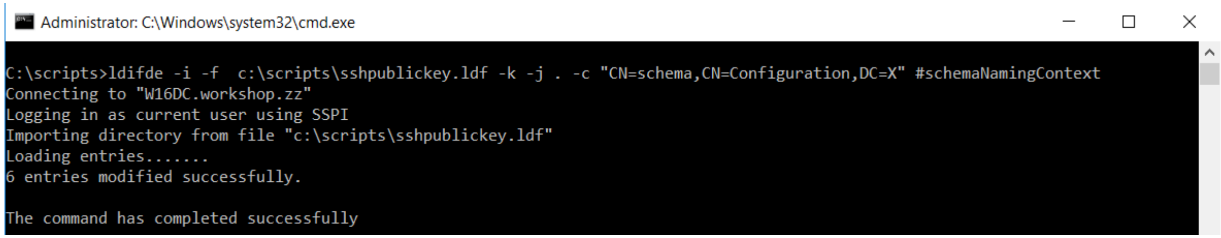
The first step is to extend your AD schema. The file sshpublickey.ldf contains the nesessary class ldapPublicKey and attribute sshPublicKey. We add the auxiliary class to the user objects. sshPublicKey is multivalued and will be replicated to Global Catalog. It is from type octet a string of bytes like in the OpenLDAP Implementation and contains an OpenSSH Public Key in the format Utf8 NoBom. The OID's are the same as in the OpenSSH LDAP environment. Thus, the AD extension is full compatible with the Open LDAP implementation. Maybe Microsoft will include it one day.

Installation
Login on a Domain Controller with an account, which is member of the Schema Admins group. Then copy the ldif file to a local path.
Execute the command:

Syntax:

```
ldifde -i -f <Path>\sshpublickey.ldf -b <username> <domain> <password> -k -j . -c
"CN=schema,CN=Configuration,DC=X" #schemaNamingContext
```

```
ldifde -i -f  c:\scripts\sshpublickey.ldf -k -j . -c "CN=schema,CN=Configuration,DC=X" #schemaNamingContext
```



```
C:\scripts>ldifde -i -f  c:\scripts\sshpublickey.ldf -k -j . -c "CN=schema,CN=Configuration,DC=X" #schemaNamingContext
Connecting to "W16DC.workshop.zz"
Logging in as current user using SSPI
Importing directory from file "c:\scripts\sshpublickey.ldf"
Loading entries.......
6 entries modified successfully.

The command has completed successfully
```

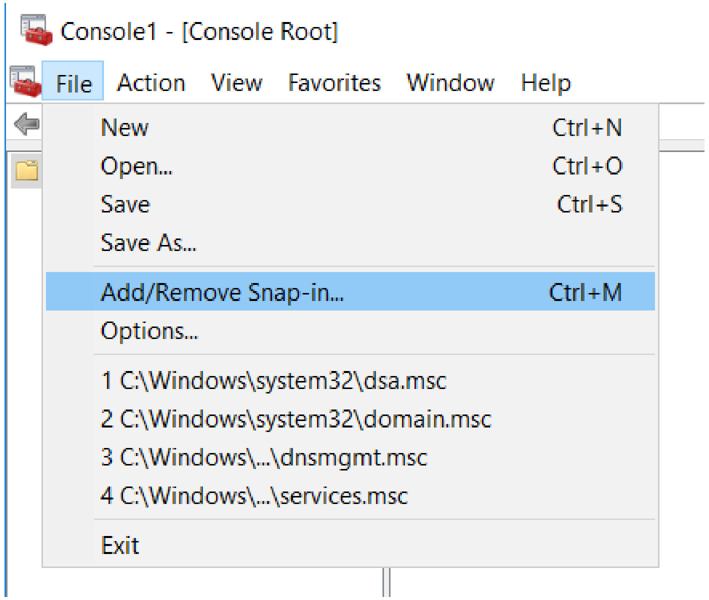
a. Examine the new Schema

You can verify the change with the Schema Editor.

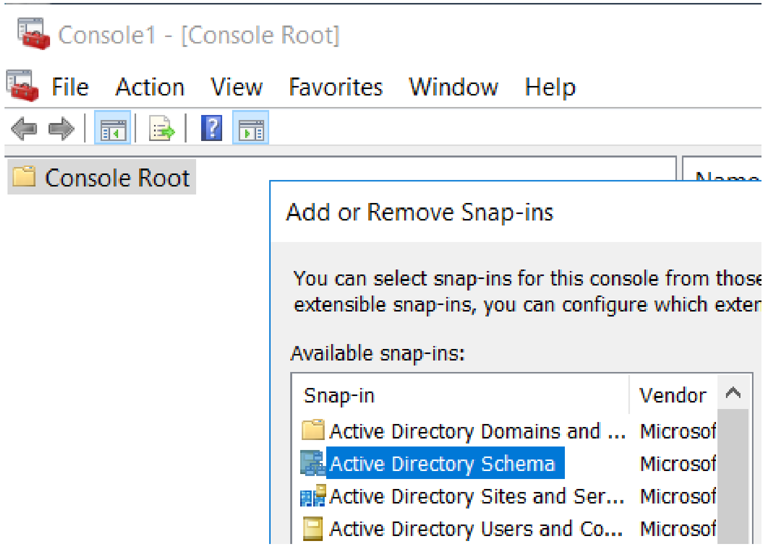
Important: Before you can using the Active Directory Schema Editor, you must register it for the first time!

```
C:\Windows\System32>regsvr32.exe schmmgmt.dll
```

Start mmc.exe in the command line (cmd.exe) and add the Snap-in "Active Directory Schema"


Console1 - [Console Root]
File
Action
View
Favorites
Window
Help
New Ctrl+N
Open... Ctrl+O
Save Ctrl+S
Save As...
Add/Remove Snap-in... Ctrl+M
Options...
1 C:\Windows\system32\dsa.msc
2 C:\Windows\system32\domain.msc
3 C:\Windows\...\dnsmgmt.msc
4 C:\Windows\...\services.msc
Exit

Add Snap-in



Add or Remove Snap-ins

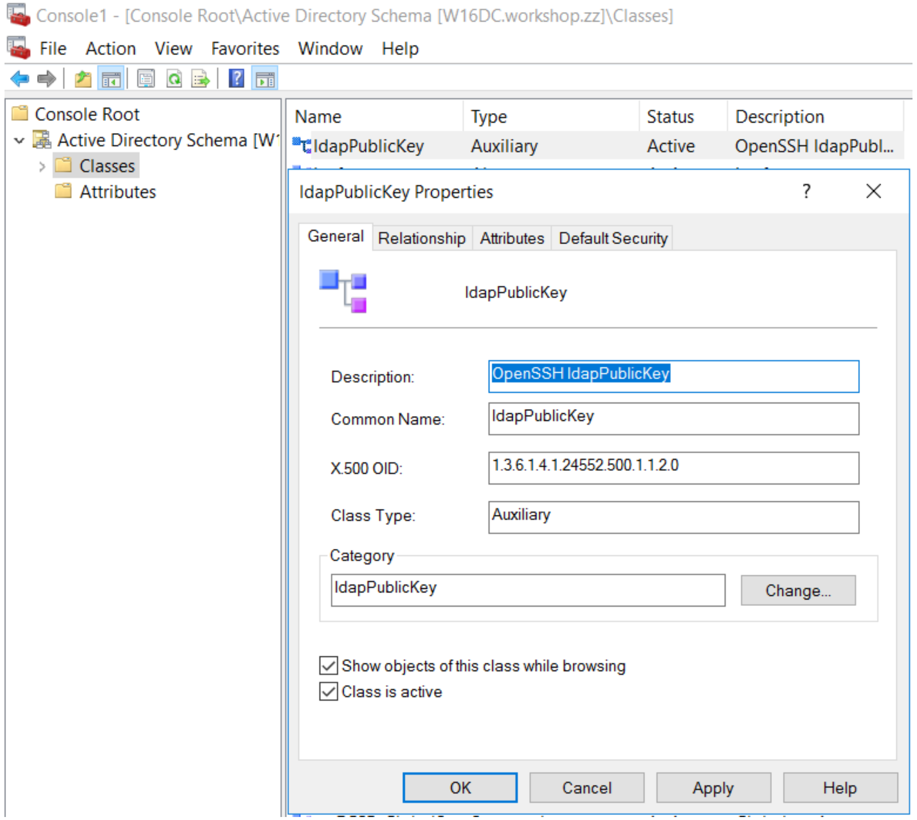
You can select snap-ins for this console from those
extensible snap-ins, you can configure which exter

Available snap-ins:

Snap-in	Vendor
Active Directory Domains and ...	Microsof
Active Directory Schema	Microsof
Active Directory Sites and Ser...	Microsof
Active Directory Users and Co...	Microsof

Select "Active Directory Schema"

Next we want exame the customize class and attribute.


Console1 - [Console Root\Active Directory Schema [W16DC.workshop.zz]\Classes]
File Action View Favorites Window Help
Console Root
Active Directory Schema [W
Classes
Attributes
General Relationship Attributes Default Security
OK Cancel Apply Help
Change...

Name	Type	Status	Description
ldapPublicKey	Auxiliary	Active	OpenSSH ldapPubl...

ldapPublicKey Properties

ldapPublicKey

Description: OpenSSH ldapPublicKey

Common Name: ldapPublicKey

X.500 OID: 1.3.6.1.4.1.24552.500.1.1.2.0

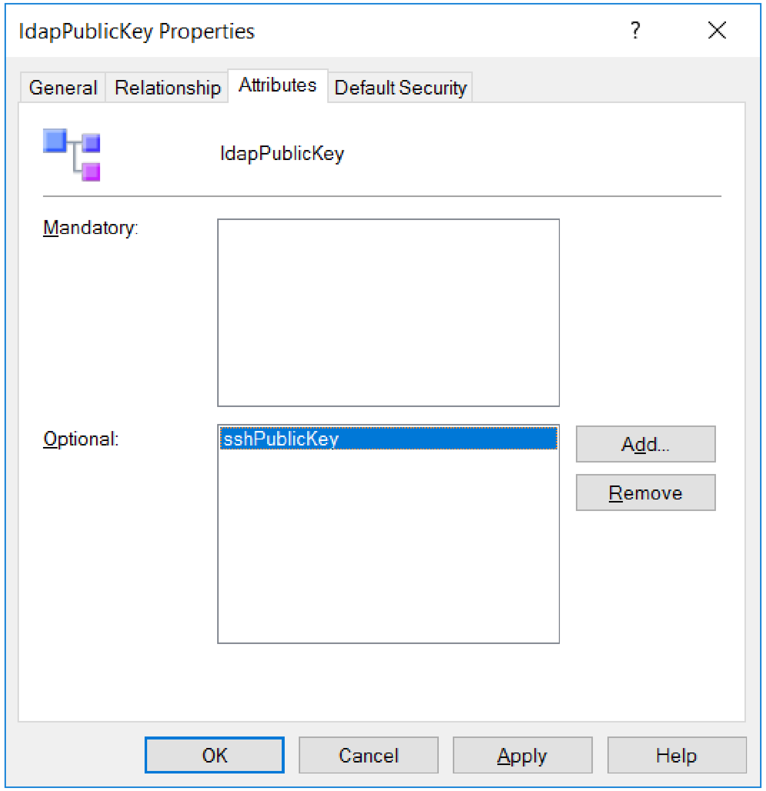
Class Type: Auxiliary

Category: ldapPublicKey

☑ Show objects of this class while browsing

☑ Class is active

Now select "Classes" and search after "ldapPublicKey" entry and select it.
You see the official OID Number and class type auxiliary.

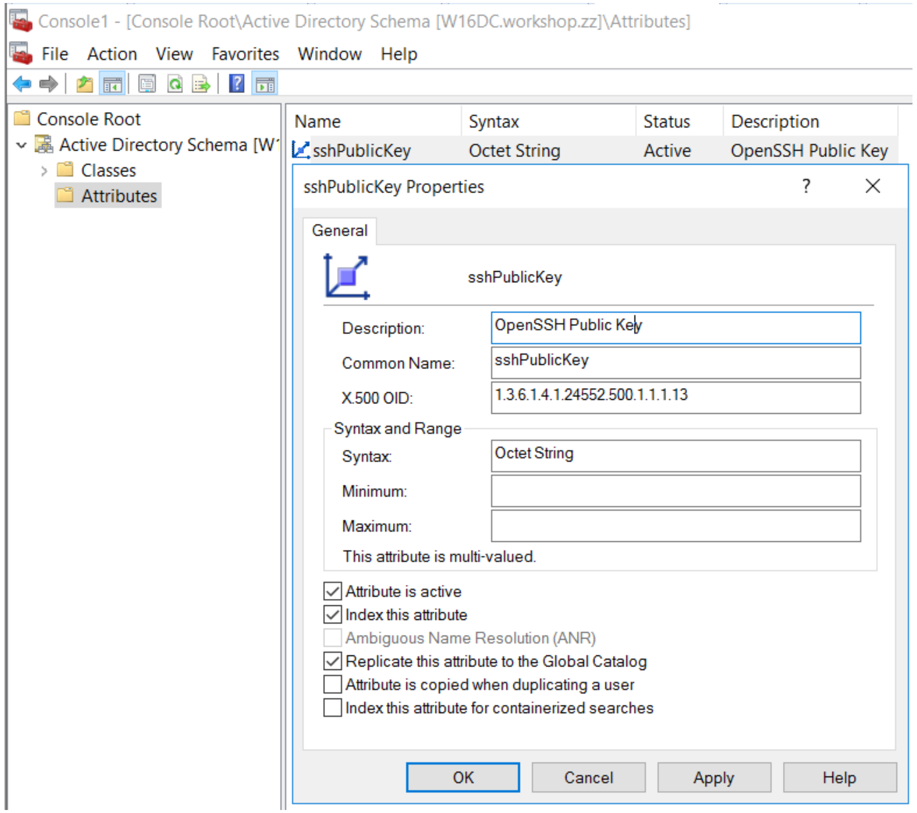


ldapPublicKey

Mandatory:

Optional: sshPublicKey

Change to Tab "Attributes"
The class includes the sshPublicKey attribute.



Name	Syntax	Status	Description
sshPublicKey	Octet String	Active	OpenSSH Public Key

sshPublicKey

Description: OpenSSH Public Key

Common Name: sshPublicKey

X.500 OID: 1.3.6.1.4.1.24552.500.1.1.1.13

Syntax and Range

Syntax: Octet String

Minimum:

Maximum:

This attribute is multi-valued.

☑ Attribute is active

☑ Index this attribute

□ Ambiguous Name Resolution (ANR)

☑ Replicate this attribute to the Global Catalog

□ Attribute is copied when duplicating a user

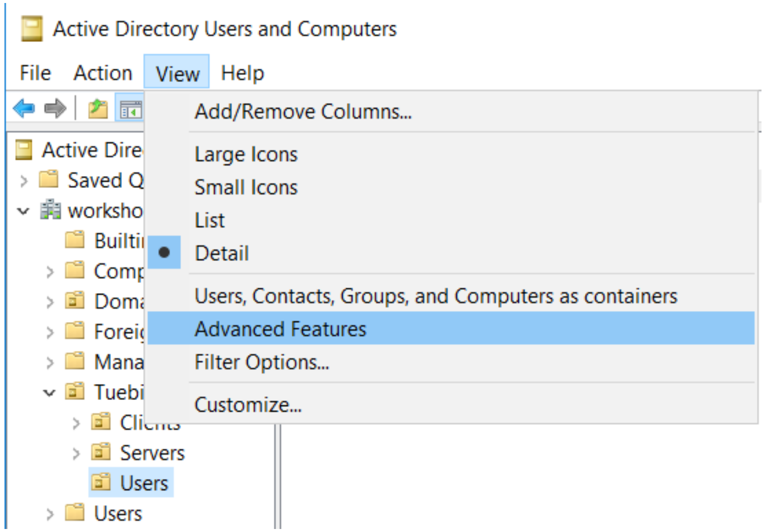
□ Index this attribute for containerized searches

Change to"Attributes" and locate "sshPublicKey" entry and select it. You see the official OID Number and the type "Octet" which means that it's a byte string. The attribute is multi-valued and indexed and will be replicated to GC.

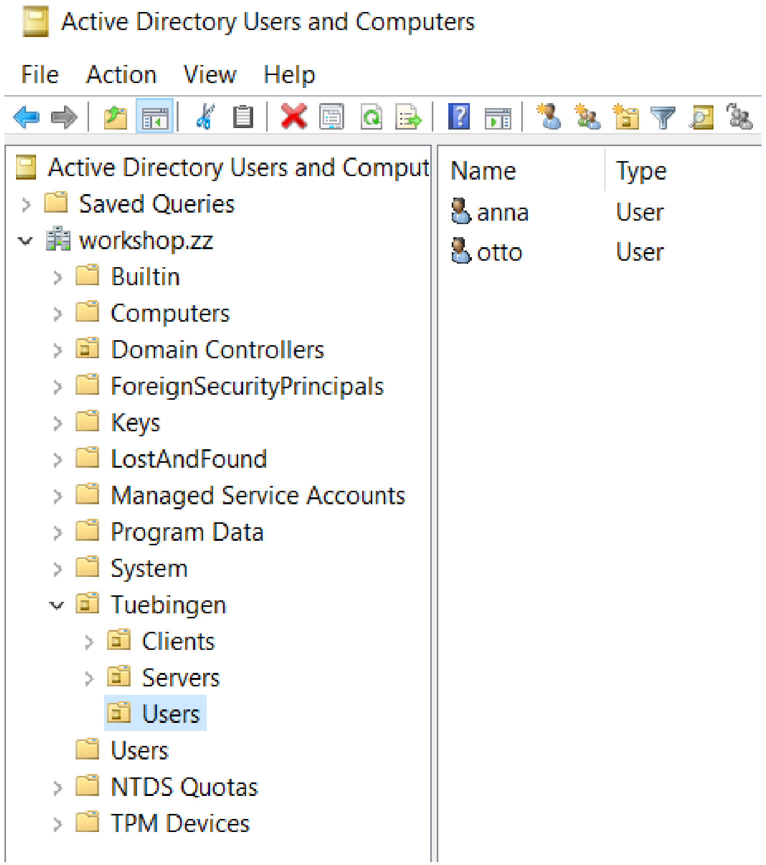
b. List and Edit the sshPublicKey Attribute of an User

We use the integrated attribute editor of "Active Directory Users and Computers" application.
Start `dsa.msc` from command line on the Domain Controller.

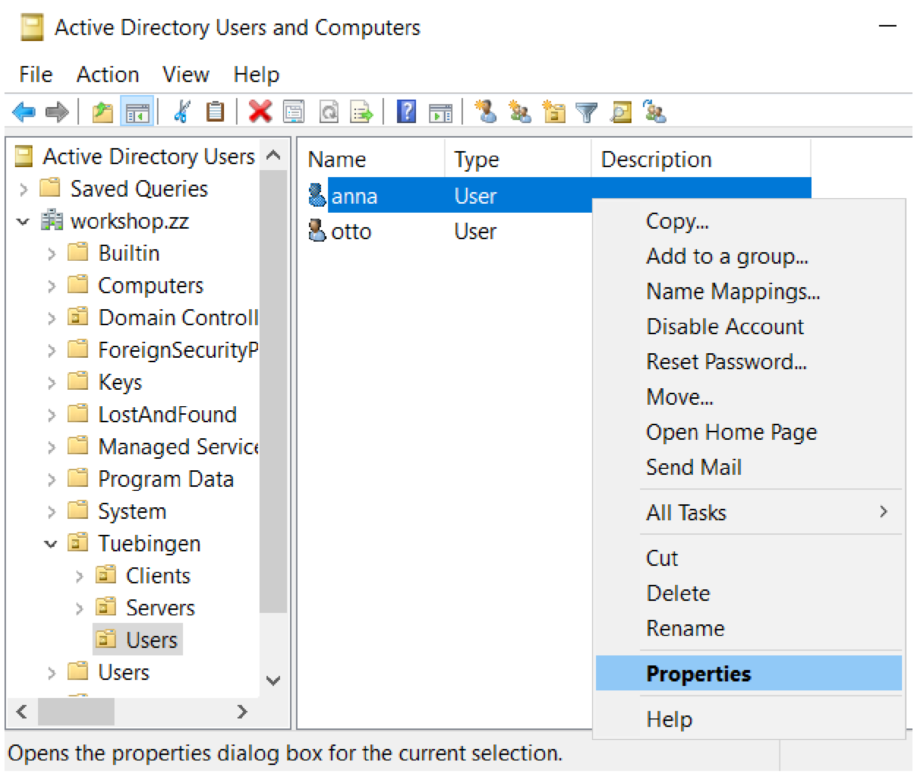
Important: Select "Advanced Features" before you select the user!



Under the view menu select "Advanced Features"



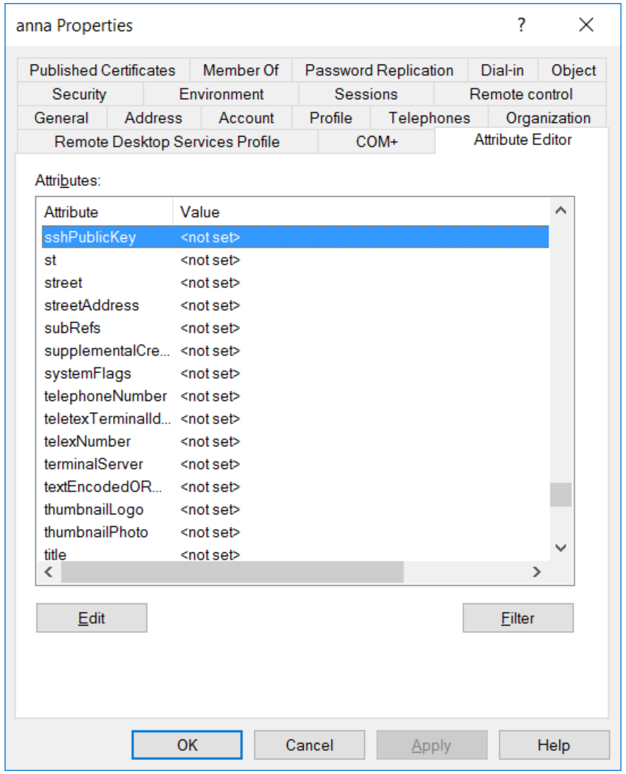
Ensure that you see more details on the left side.



Name	Type	Description
anna	User	
otto	User	

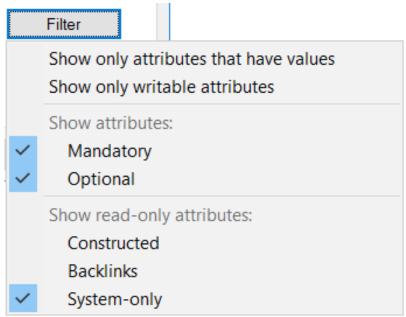
Opens the properties dialog box for the current selection.

Right click on the user and select "Properties".



Attribute	Value
sshPublicKey	<not set>
st	<not set>
street	<not set>
streetAddress	<not set>
subRefs	<not set>
supplementalCre...	<not set>
systemFlags	<not set>
telephoneNumber	<not set>
teletexTerminalId...	<not set>
telexNumber	<not set>
terminalServer	<not set>
textEncodedOR...	<not set>
thumbnailLogo	<not set>
thumbnailPhoto	<not set>
title	<not set>

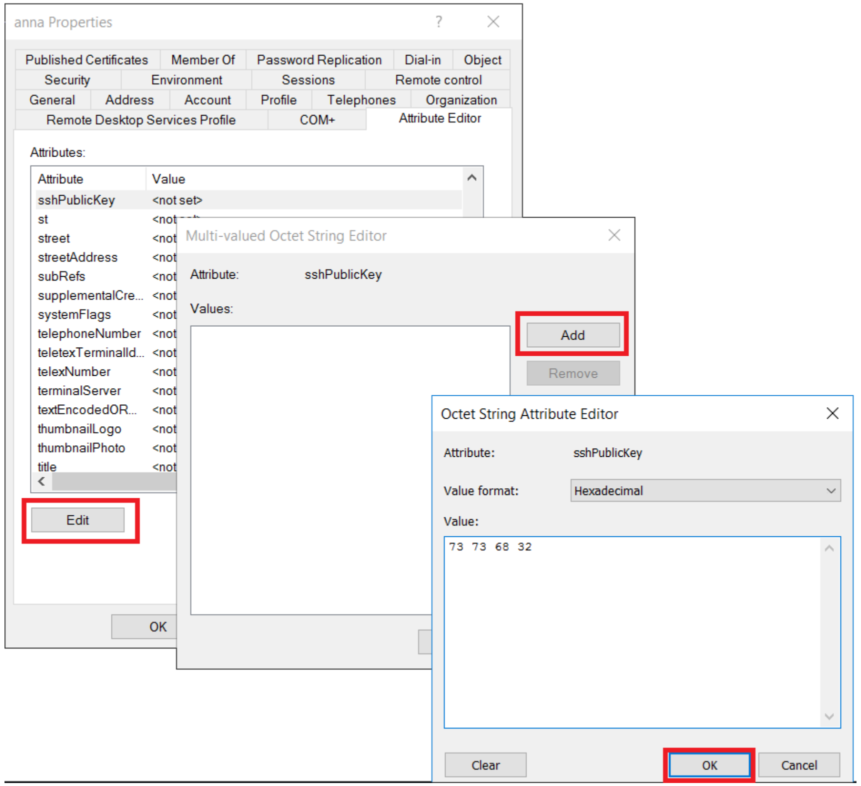
Select the tab "Attribute Editor"
Search after "sshPublicKey".



Show only attributes that have values
Show only writable attributes
Show attributes:
✓ Mandatory
✓ Optional
Show read-only attributes:
Constructed
Backlinks
✓ System-only

If you don’t find it please click the filter button on the right side and check the filter options.

Now we add a string for testing.



anna Properties

Attributes:

Attribute	Value
sshPublicKey	<not set>
st	<not
street	<not
streetAddress	<not
subRefs	<not
supplementalCre...	<not
systemFlags	<not
telephoneNumber	<not
teletexTerminalId...	<not
telexNumber	<not
terminalServer	<not
textEncodedOR...	<not
thumbnailLogo	<not
thumbnailPhoto	<not
title	<not

Multi-valued Octet String Editor

Attribute: sshPublicKey

Values:

Octet String Attribute Editor

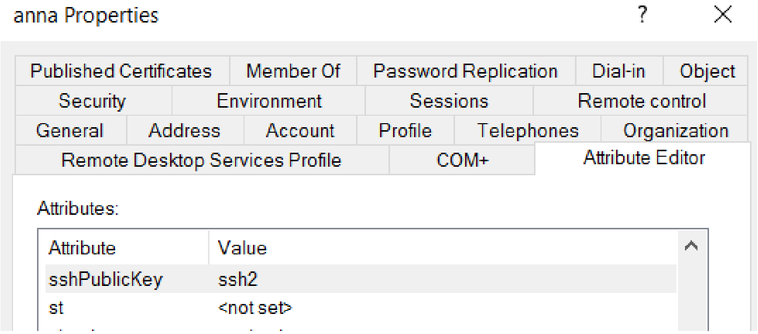
Attribute: sshPublicKey

Value format: Hexadecimal

Value:

```
73 73 68 32
```

Select the key. Then click on the "Edit" and the "Add" button. By default the value format is set to hex. Insert the byte code of the string. Finally hit the "OK" button two times.



anna Properties

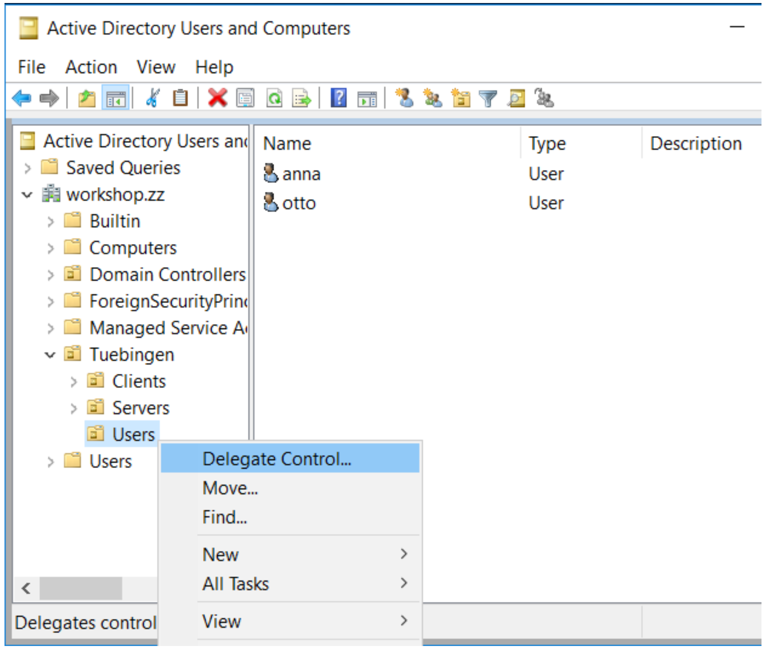
Attributes:

Attribute	Value
sshPublicKey	ssh2
st	<not set>

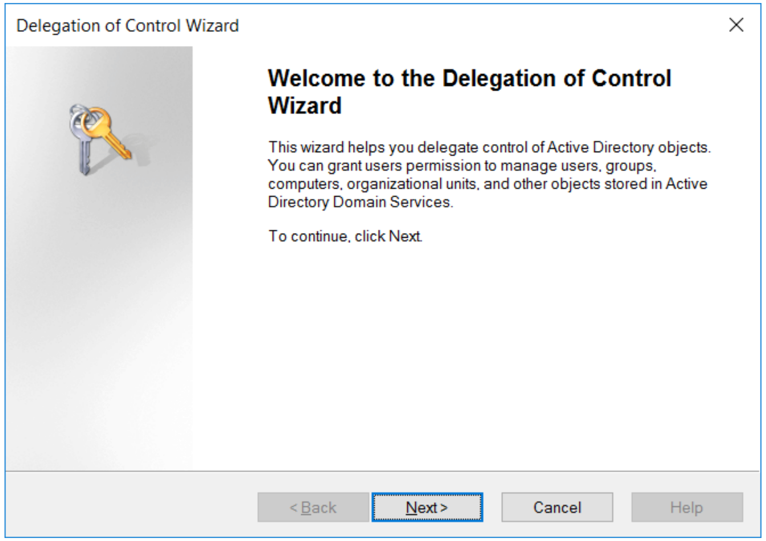
The entered string appears.

2. Making the Attribute accessible for Self-Service

This procedure is optional. If you want allow that your users itself can change the sshPublicKey you must give them "NT Authority\Self" rights. To achieve this you must delegate the organization unit and you need Domain Admin rights.



A delegation wizard will start.

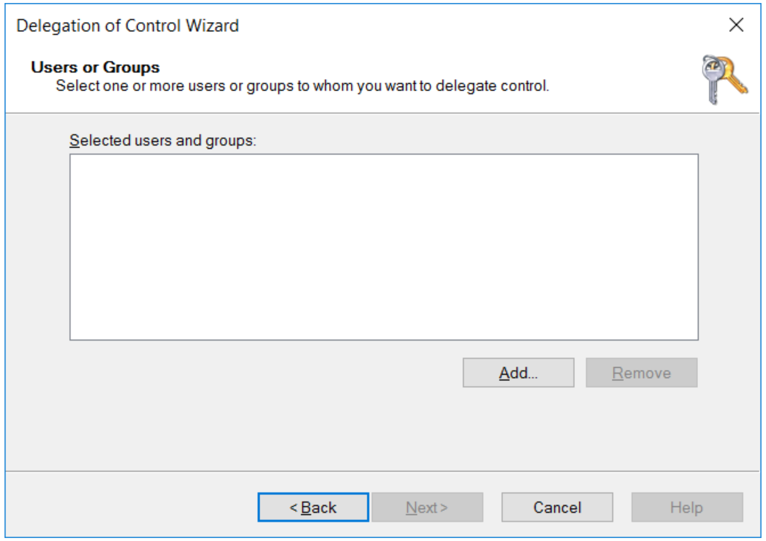

Delegation of Control Wizard

Welcome to the Delegation of Control Wizard

This wizard helps you delegate control of Active Directory objects. You can grant users permission to manage users, groups, computers, organizational units, and other objects stored in Active Directory Domain Services.

To continue, click Next.

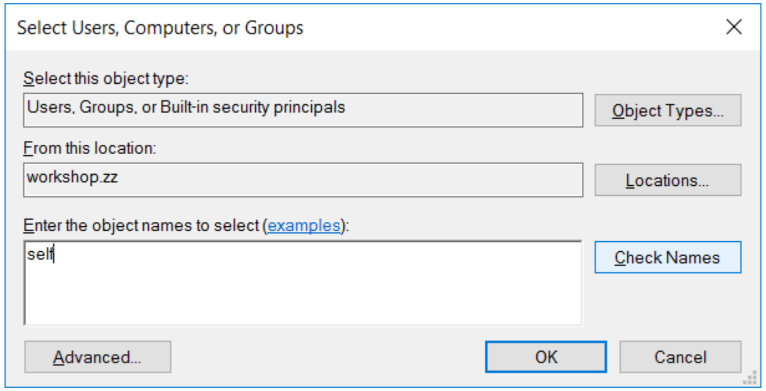
Click "Next" button


Delegation of Control Wizard

Users or Groups
Select one or more users or groups to whom you want to delegate control.

Selected users and groups:

Click "Add" button

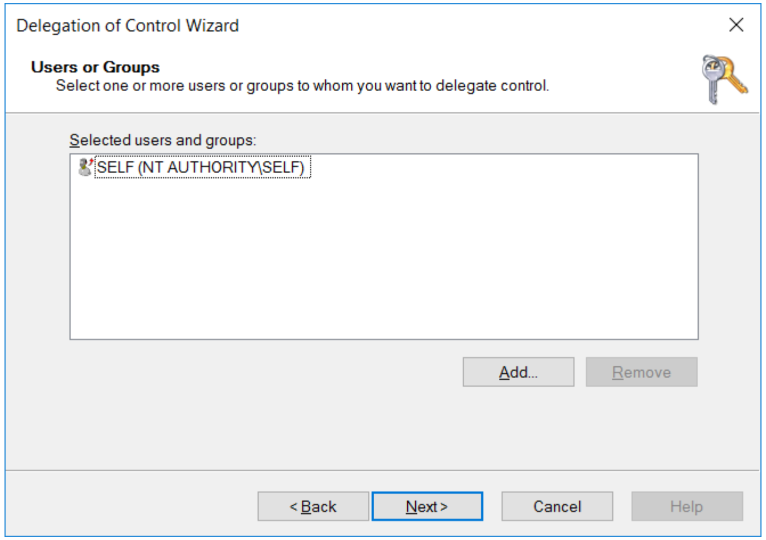

Select Users, Computers, or Groups

Select this object type:
Users, Groups, or Built-in security principals

From this location:
workshop.zz

Enter the object names to select (examples):
self

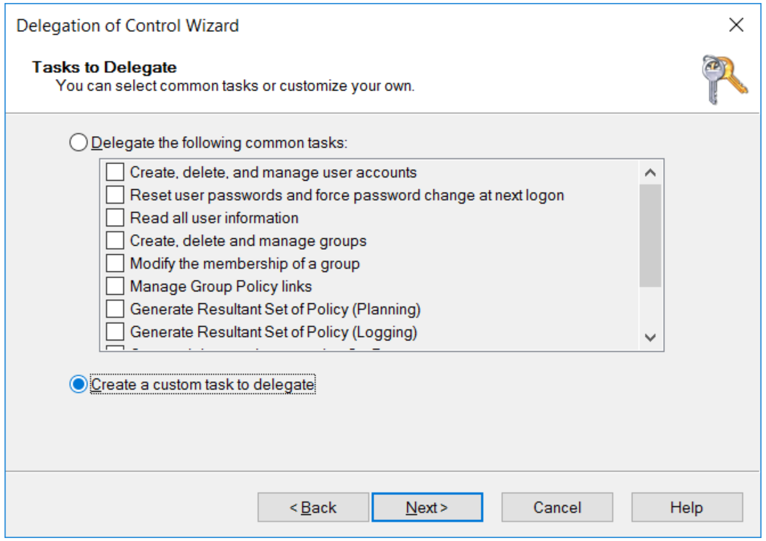
Enter `self` and click button "Check Names".
Self will be underlined. Complete this step with OK.


Delegation of Control Wizard

Users or Groups
Select one or more users or groups to whom you want to delegate control.

Selected users and groups:
SELF (NT AUTHORITY\SELF)

Click "Next" button



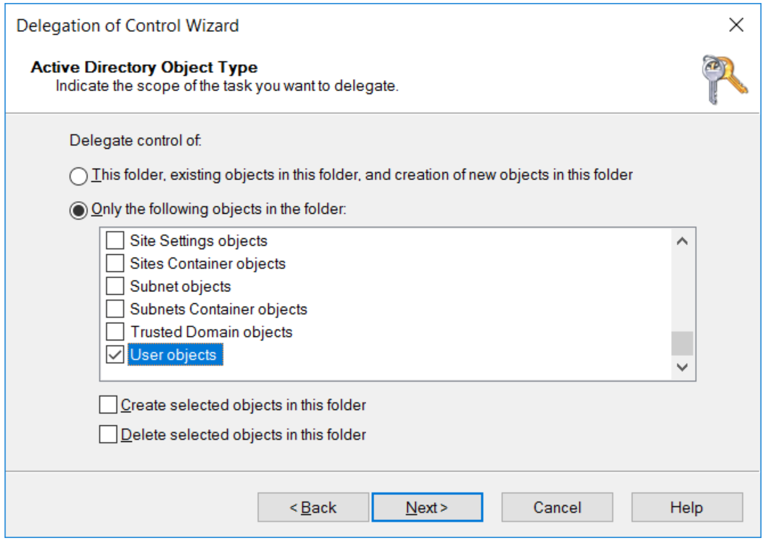
Tasks to Delegate
You can select common tasks or customize your own.

○ Delegate the following common tasks:

- □ Create, delete, and manage user accounts
- □ Reset user passwords and force password change at next logon
- □ Read all user information
- □ Create, delete and manage groups
- □ Modify the membership of a group
- □ Manage Group Policy links
- □ Generate Resultant Set of Policy (Planning)
- □ Generate Resultant Set of Policy (Logging)

● Create a custom task to delegate

Select the radio button "Create a custom task to delegate" and then button "Next"



Active Directory Object Type
Indicate the scope of the task you want to delegate.

Delegate control of:

○ This folder, existing objects in this folder, and creation of new objects in this folder

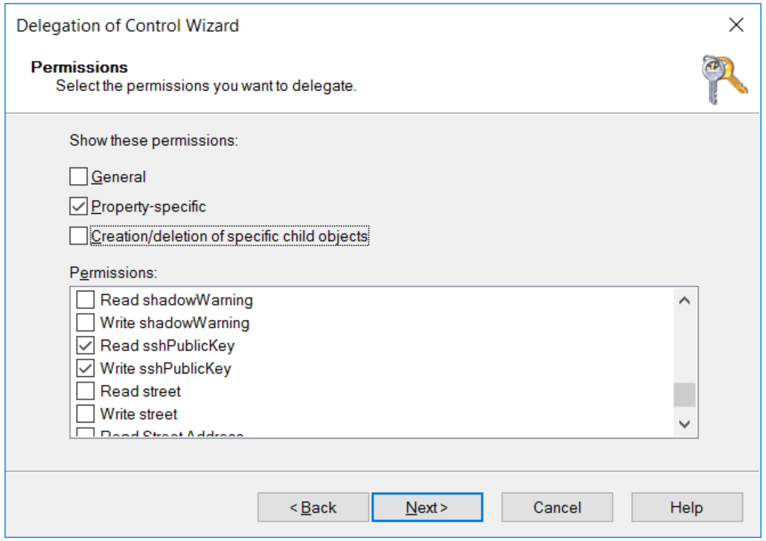
● Only the following objects in the folder:

- □ Site Settings objects
- □ Sites Container objects
- □ Subnet objects
- □ Subnets Container objects
- □ Trusted Domain objects
- ☑ User objects

□ Create selected objects in this folder

□ Delete selected objects in this folder

Select the option "Only the following objects in the folder". Scroll down and choose "User objects"



Permissions
Select the permissions you want to delegate.

Show these permissions:

□ General

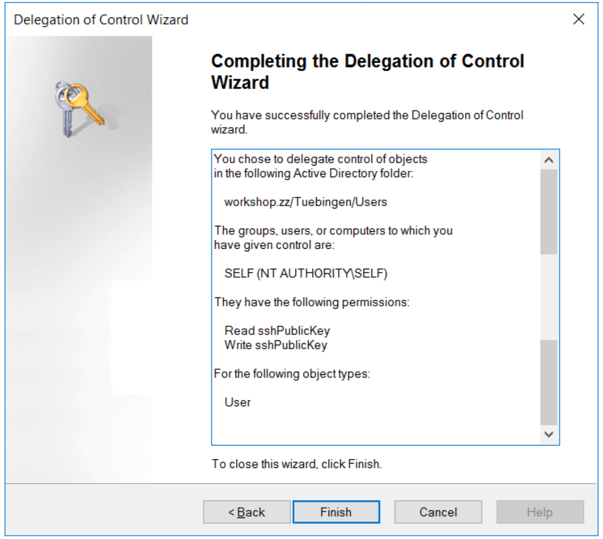
☑ Property-specific

□ Creation/deletion of specific child objects

Permissions:

- □ Read shadowWarning
- □ Write shadowWarning
- ☑ Read sshPublicKey
- ☑ Write sshPublicKey
- □ Read street
- □ Write street
- □ Read Street Address

Select Property-specific and search after the "sshPublicKey" entries. Select both "Read sshPublicKey" and "Write sshPublicKey" option.



Completing the Delegation of Control Wizard

You have successfully completed the Delegation of Control wizard.

You chose to delegate control of objects
in the following Active Directory folder:

workshop.zz/Tuebingen/Users

The groups, users, or computers to which you
have given control are:

SELF (NT AUTHORITY\SELF)

They have the following permissions:

Read sshPublicKey
Write sshPublicKey

For the following object types:

User

To close this wizard, click Finish.

A summary of the selected delegation occurs. Complete it with the "Finish" button

3. Testing of the PowerShell Script ssh-ad-pubkey

Test the PowerShell script ssh-ad-pubkey.ps1. It run's with Windows PowerShell 2.0-5.1 and PowerShell Core 6.x on Windows. It requires .Net Framework 3.5. The PowerShell Core version needs to work the PSCoreWindowsCompat module.

See
https://github.com/markekraus/PSCoreWindowsCompat

Help:

```
.\ssh-ad-pubkey.ps1 -?
```

More Help

```
Get-Help .\ssh-ad-pubkey.ps1 -full
```

Syntax:

```
PS C:\scripts> get-command .\ssh-ad-pubkey.ps1 -Syntax

ssh-ad-pubkey.ps1 [<CommonParameters>]
ssh-ad-pubkey.ps1 -list [[-sam] <string>] [<CommonParameters>]
ssh-ad-pubkey.ps1 -list -filepath <string> [<CommonParameters>]
ssh-ad-pubkey.ps1 -add [-filepath] <string> [[-sam] <string>] [<CommonParameters>]
ssh-ad-pubkey.ps1 -add [-sshpubkey] <string> [[-sam] <string>] [<CommonParameters>]
ssh-ad-pubkey.ps1 -remove [-filepath] <string> [[-sam] <string>] [<CommonParameters>]
ssh-ad-pubkey.ps1 -remove [-sshpubkey] <string> [[-sam] <string>] [<CommonParameters>]
ssh-ad-pubkey.ps1 -clear [[-sam] <string>] [<CommonParameters>]
ssh-ad-pubkey.ps1 -check [<CommonParameters>]
```

Examples:

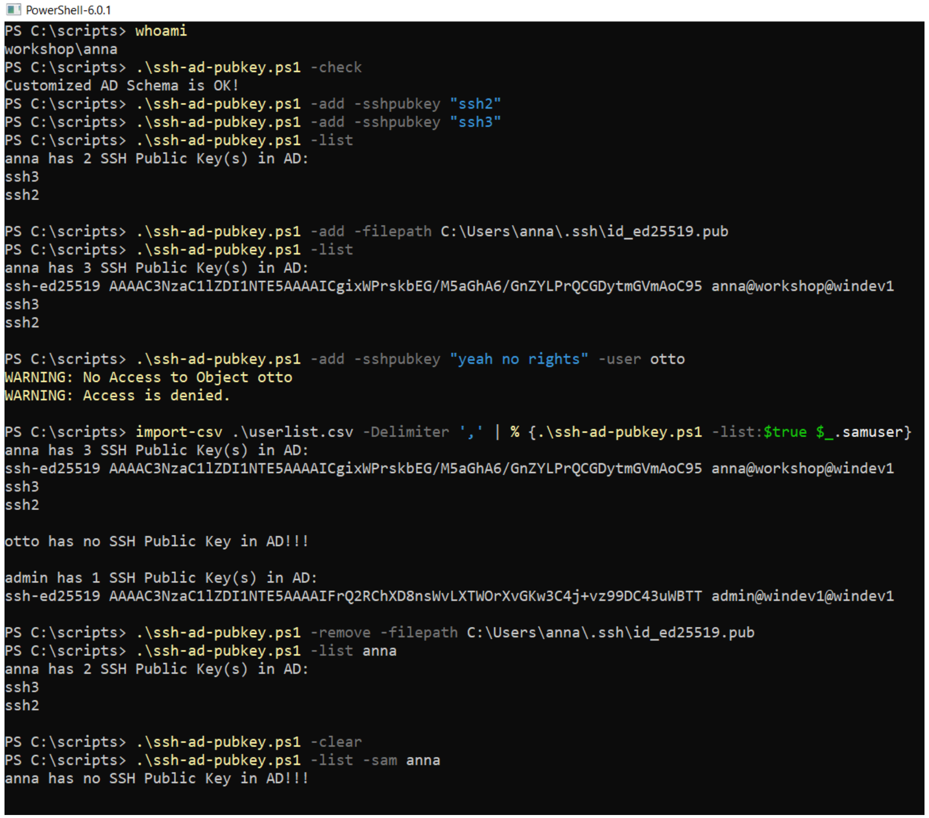
```
Get-Help .\ssh-ad-pubkey.ps1 -examples

NAME
    C:\scripts\ssh-ad-pubkey.ps1
SYNOPSIS
    Manage Ssh Public Key in Active Directory.
    -------------------------- EXAMPLE 1 --------------------------
    PS C:\>ssh-ad-pubkey -list
    List the SSH Public Key(s) for the current user.
```

```
-------------------------- EXAMPLE 2 --------------------------
PS C:\>ssh-ad-pubkey -list anna
PS C:\>ssh-ad-pubkey -list -sam  anna
PS C:\>ssh-ad-pubkey -list -user anna
List the SSH Public Key(s) for the user with SamAccountName Anna.

-------------------------- EXAMPLE 3 --------------------------
PS C:\>ssh-ad-pubkey -list -filepath C:\Users\anna\.ssh\id_ed25519.pub
List the SSH Public Key in File

-------------------------- EXAMPLE 4 --------------------------
PS C:\>ssh-ad-pubkey -add -filepath C:\Users\anna\.ssh\id_ed25519.pub
Add SSH Public Key in File to AD for current user

PS C:\>ssh-ad-pubkey -add -filepath C:\common\id_ed25519.pub -sam otto
Add SSH Public Key in File to AD for user otto

-------------------------- EXAMPLE 5 --------------------------
PS C:\>ssh-ad-pubkey -add -sshpubkey "ssh-ed25519 AAAAC3NzaC1lZD/GnZYLGmAoC95 anna@workshop@windev1"
Add SSH Public Key from Console to AD for current user

PS C:\>ssh-ad-pubkey -add -sshpubkey "ssh-ed25519 AAAAC3NzaC1lZDgixWPrskbEG42 otto@workshop@windev1" -sam otto
Add SSH Public Key from Console to AD for user otto

-------------------------- EXAMPLE 6 --------------------------
PS C:\>ssh-ad-pubkey -remove -filepath C:\Users\anna\.ssh\id_ed25519.pub
Remove SSH Public Key in File from AD for current user

PS C:\>ssh-ad-pubkey -remove -filepath C:\common\id_ed25519.pub -sam otto
Remove SSH Public Key in File from AD for user otto

-------------------------- EXAMPLE 7 --------------------------
PS C:\>ssh-ad-pubkey -remove -sshpubkey "ssh-ed25519 AAAAC3NzaC1lZD/GnZYLGmAoC95 anna@workshop@windev1"
Remove SSH Public Key from Console from AD for current user

PS C:\>ssh-ad-pubkey -remove -sshpubkey "ssh-ed25519 AAAAC3NzaC1lZDgixWPrskbEG42 otto@workshop@windev1" -sam otto
Remove SSH Public Key from Console from AD for user otto
```

```
-------------------------- EXAMPLE 8 --------------------------
PS C:\>ssh-ad-pubkey –clear
Clear all SSH Public Keys from AD for current user

PS C:\>ssh-ad-pubkey -clear -sam otto
Clear all SSH Public Key from AD for user otto

-------------------------- EXAMPLE 9 --------------------------
PS C:\>ssh-add-pubkey –check
Check the AD schema for the required extentions for OpenSSH

-------------------------- EXAMPLE 10 --------------------------
PS c:\>import-csv .\userlist.csv -Delimiter ',' | % {.\ssh-ad-pubkey.ps1 -list:$true $_.sam}
List the SSH Public Key stored in Active Directory from all Users defined in a comma separated file.
```

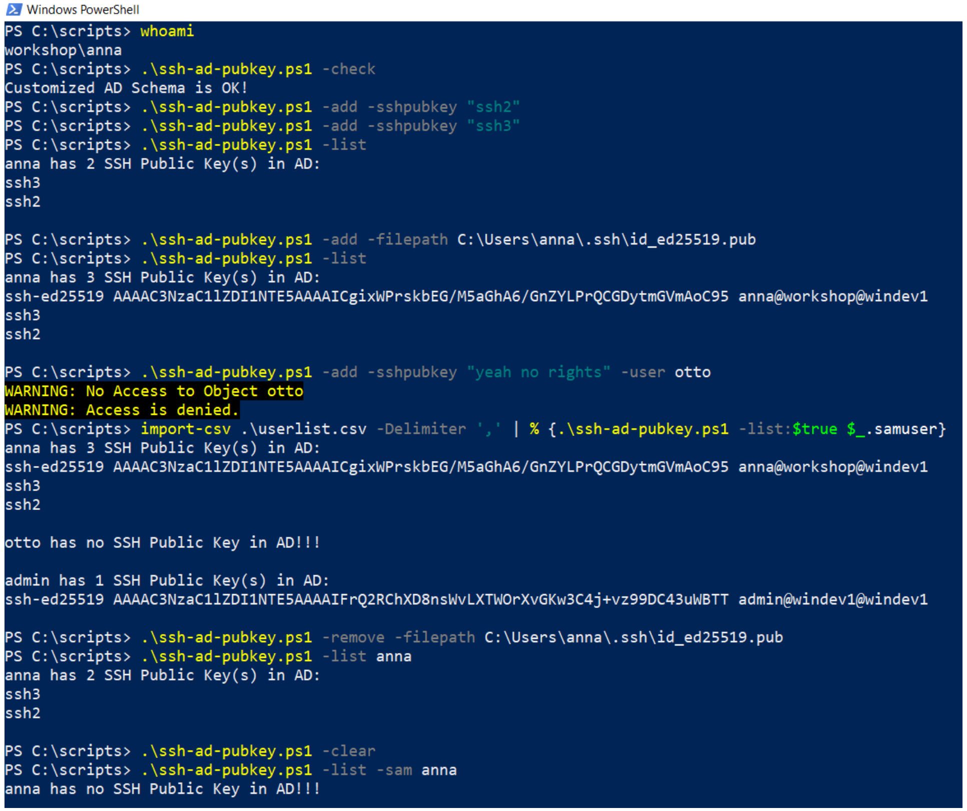
Testing

Test with PowerShell Core 6.x



```
PS C:\scripts> whoami
workshop\anna
PS C:\scripts> .\ssh-ad-pubkey.ps1 -check
Customized AD Schema is OK!
PS C:\scripts> .\ssh-ad-pubkey.ps1 -add -sshpubkey "ssh2"
PS C:\scripts> .\ssh-ad-pubkey.ps1 -add -sshpubkey "ssh3"
PS C:\scripts> .\ssh-ad-pubkey.ps1 -list
anna has 2 SSH Public Key(s) in AD:
ssh3
ssh2

PS C:\scripts> .\ssh-ad-pubkey.ps1 -add -filepath C:\Users\anna\.ssh\id_ed25519.pub
PS C:\scripts> .\ssh-ad-pubkey.ps1 -list
anna has 3 SSH Public Key(s) in AD:
ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAICgixWPrskbEG/M5aGhA6/GnZYLPrQCGDytmGVmAoC95 anna@workshop@windev1
ssh3
ssh2

PS C:\scripts> .\ssh-ad-pubkey.ps1 -add -sshpubkey "yeah no rights" -user otto
WARNING: No Access to Object otto
WARNING: Access is denied.

PS C:\scripts> import-csv .\userlist.csv -Delimiter ',' | % {.\ssh-ad-pubkey.ps1 -list:$true $_.samuser}
anna has 3 SSH Public Key(s) in AD:
ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAICgixWPrskbEG/M5aGhA6/GnZYLPrQCGDytmGVmAoC95 anna@workshop@windev1
ssh3
ssh2

otto has no SSH Public Key in AD!!!

admin has 1 SSH Public Key(s) in AD:
ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIFrQ2RChXD8nsWvLXTWOrXvGKw3C4j+vz99DC43uWBTT admin@windev1@windev1

PS C:\scripts> .\ssh-ad-pubkey.ps1 -remove -filepath C:\Users\anna\.ssh\id_ed25519.pub
PS C:\scripts> .\ssh-ad-pubkey.ps1 -list anna
anna has 2 SSH Public Key(s) in AD:
ssh3
ssh2

PS C:\scripts> .\ssh-ad-pubkey.ps1 -clear
PS C:\scripts> .\ssh-ad-pubkey.ps1 -list -sam anna
anna has no SSH Public Key in AD!!!
```

Test with Windows PowerShell 5.1



```
PS C:\scripts> whoami
workshop\anna
PS C:\scripts> .\ssh-ad-pubkey.ps1 -check
Customized AD Schema is OK!
PS C:\scripts> .\ssh-ad-pubkey.ps1 -add -sshpubkey "ssh2"
PS C:\scripts> .\ssh-ad-pubkey.ps1 -add -sshpubkey "ssh3"
PS C:\scripts> .\ssh-ad-pubkey.ps1 -list
anna has 2 SSH Public Key(s) in AD:
ssh3
ssh2

PS C:\scripts> .\ssh-ad-pubkey.ps1 -add -filepath C:\Users\anna\.ssh\id_ed25519.pub
PS C:\scripts> .\ssh-ad-pubkey.ps1 -list
anna has 3 SSH Public Key(s) in AD:
ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAICgixWPrskbEG/M5aGhA6/GnZYLPrQCGDytmGVmAoC95 anna@workshop@windev1
ssh3
ssh2

PS C:\scripts> .\ssh-ad-pubkey.ps1 -add -sshpubkey "yeah no rights" -user otto
WARNING: No Access to Object otto
WARNING: Access is denied.
PS C:\scripts> import-csv .\userlist.csv -Delimiter ',' | % {.\ssh-ad-pubkey.ps1 -list:$true $_.samuser}
anna has 3 SSH Public Key(s) in AD:
ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAICgixWPrskbEG/M5aGhA6/GnZYLPrQCGDytmGVmAoC95 anna@workshop@windev1
ssh3
ssh2

otto has no SSH Public Key in AD!!!

admin has 1 SSH Public Key(s) in AD:
ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIFrQ2RChXD8nsWvLXTWOrXvGKw3C4j+vz99DC43uWBTT admin@windev1@windev1

PS C:\scripts> .\ssh-ad-pubkey.ps1 -remove -filepath C:\Users\anna\.ssh\id_ed25519.pub
PS C:\scripts> .\ssh-ad-pubkey.ps1 -list anna
anna has 2 SSH Public Key(s) in AD:
ssh3
ssh2

PS C:\scripts> .\ssh-ad-pubkey.ps1 -clear
PS C:\scripts> .\ssh-ad-pubkey.ps1 -list -sam anna
anna has no SSH Public Key in AD!!!
```