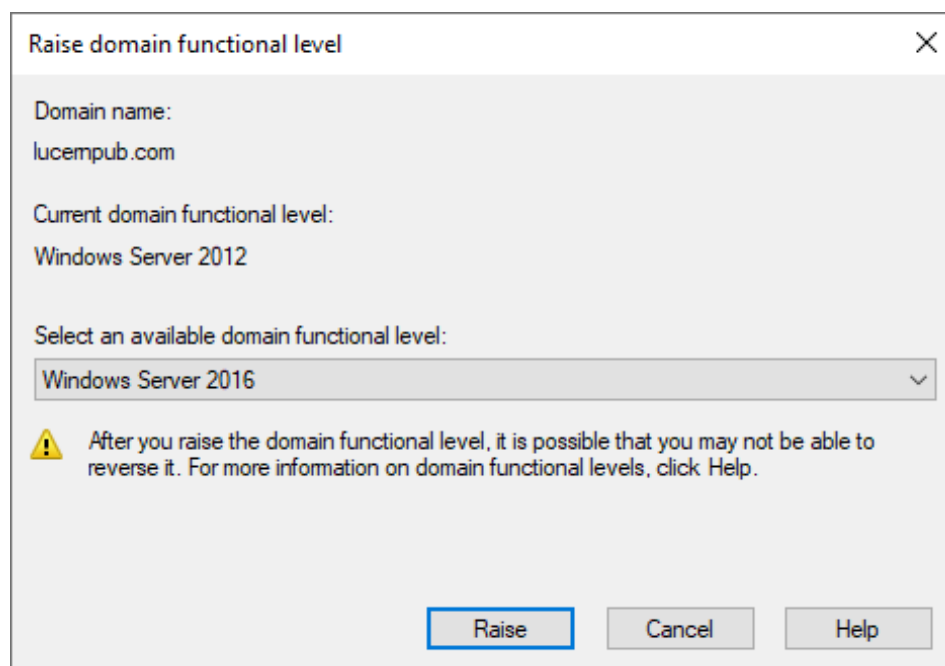
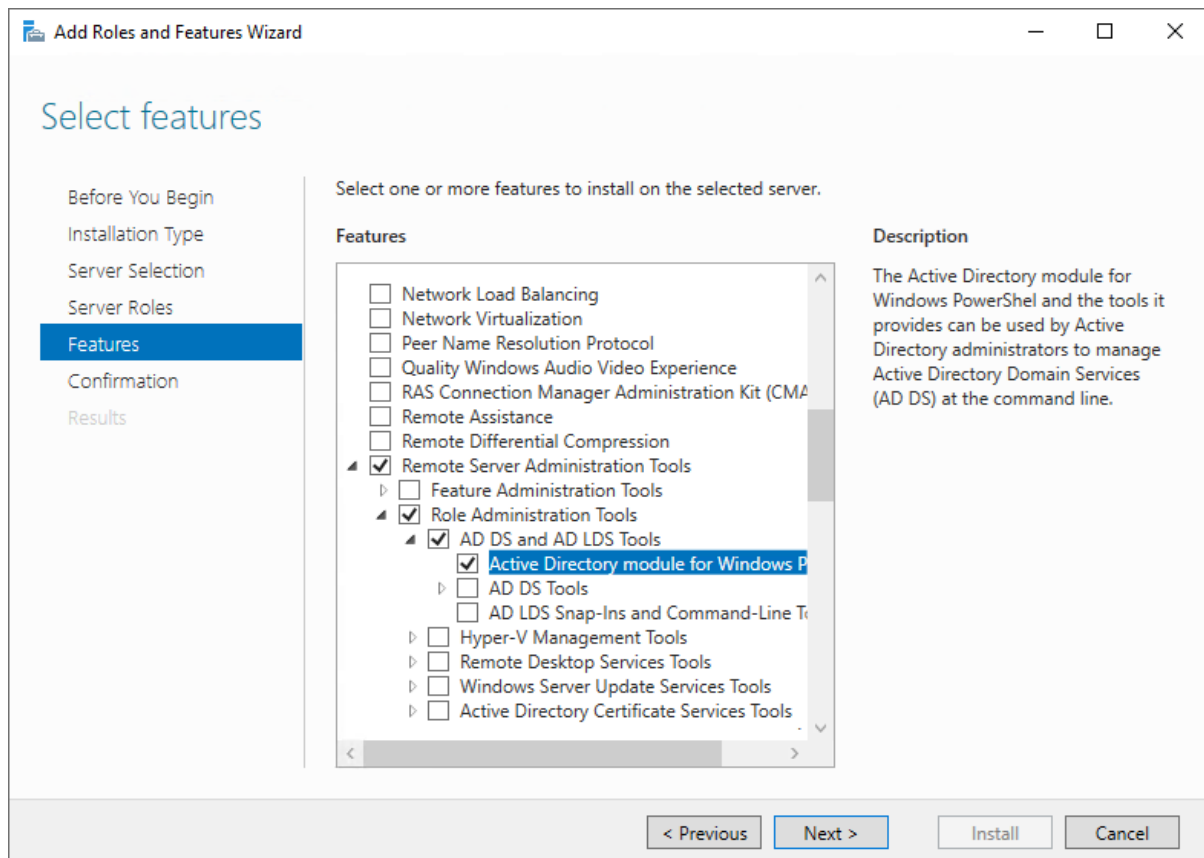


Chapter 1: Optimizing Forests, Domains, and Trusts



Raise forest functional level

Forest name:
lucempub.com

Current forest functional level:
Windows Server 2012

Select an available forest functional level:
Windows Server 2016

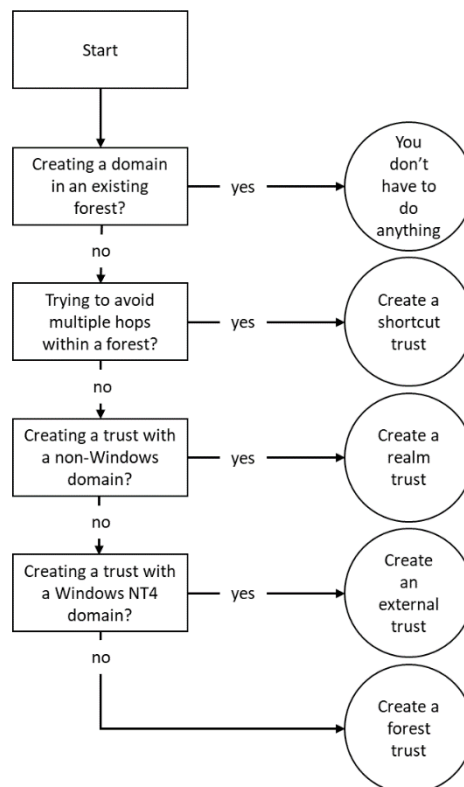
⚠

After you raise the forest functional level, it is possible that you may not be able to reverse it. For more information on forest functional levels, click Help.

Raise

Cancel

Help



lucernpub.com Properties

General Trusts Managed By

Domains trusted by this domain (outgoing trusts):

Domain Name	Trust Type	Transitive
-------------	------------	------------

Properties...
Remove

Domains that trust this domain (incoming trusts):

Domain Name	Trust Type	Transitive
-------------	------------	------------

Properties...
Remove

New Trust...

OK Cancel Apply Help

New Trust Wizard

Trust Creation Complete
The trust relationship was successfully created.

Status of changes:

Trust relationship created successfully.
Specified domain: wuhanpub.com

Direction:
Two-way: Users in the local domain can authenticate in the specified domain and users in the specified domain can authenticate in the local domain.

Trust type: Forest trust

Outgoing trust authentication level: Forest-wide authentication in local and specified forests.

To configure the new trust, click Next.

< Back Next > Cancel

lucernpub.com Properties ? X

General Name Suffix Routing Authentication

This Domain:

Other Domain:

Trust type:

☐ The other domain supports Kerberos AES Encryption

Direction of trust:

Two-way: Users in the local domain can authenticate in the specified domain and users in the specified domain can authenticate in the local domain.

Transitivity of trust:

This trust is forest transitive. Users from indirectly trusted domains within the enterprise may authenticate in the trusting enterprise.

To confirm or reset this trust relationship and update its routed name suffixes, click Validate.

To save a file with the details about the status of the names associated with this trust, click Save As.

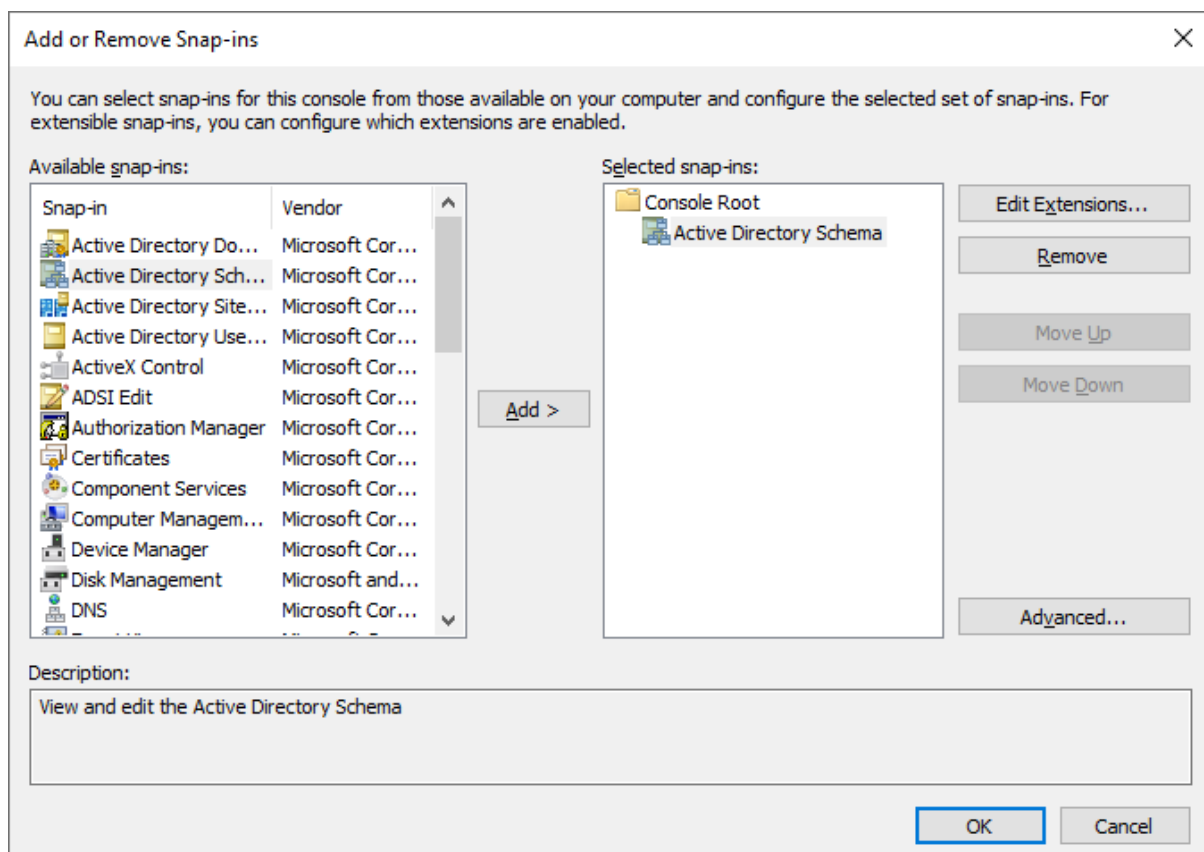
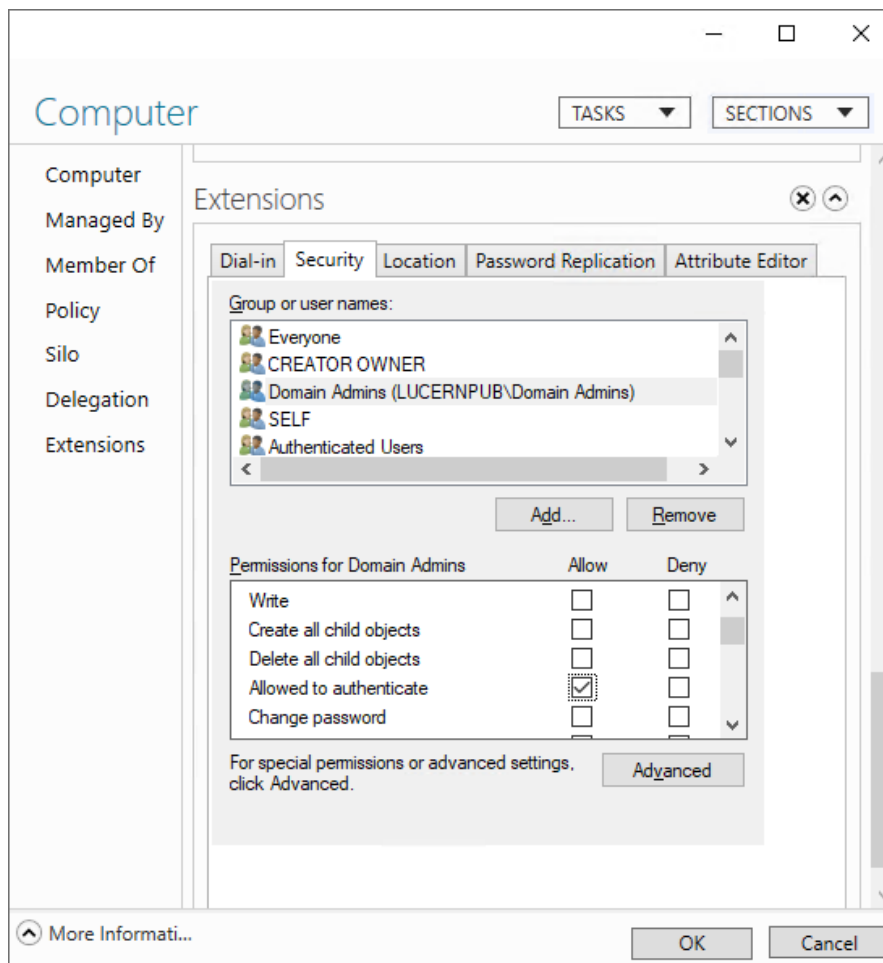
lucernpub.com Properties ? X

General Name Suffix Routing Authentication

Select the scope of authentication for users in the lucernpub.com forest.


☒ Forest-wide authentication
Windows will automatically authenticate users from the specified forest for all resources in the local forest. This option is preferred when both forests belong to the same organization.

☐ Selective authentication
Windows will not automatically authenticate users from the specified forest for any resources in the local forest. After you close this dialog, grant individual access to each domain and server that you want to make available to users in the specified forest. This option is preferred if the forests belong to different organizations.



Schema Object Creation

×




WARNING: Creating schema objects is a permanent operation. While these objects may be disabled to prevent their usage, they can not be deleted and will become a permanent part of your enterprise installation.

Continue

Cancel

Create New Attribute

×



Create a New Attribute Object

Identification

Common Name:

LDAP Display Name:

Unique X500 Object ID:

Description:

Syntax and Range

Syntax:

Access Point

Minimum:

Maximum:

☐ Multi-Valued

OK

Cancel

Help

Create New Schema Class

Identification

Common Name:

LDAP Display Name:

Unique X500 Object ID:

Description:

Inheritance and Type

Parent Class:

Class Type:

Structural


< Back

Next >

Cancel

Help

Enable Recycle Bin Confirmation




Are you sure you want to perform this action? Once Recycle Bin has been enabled, it cannot be disabled.

OK

Cancel

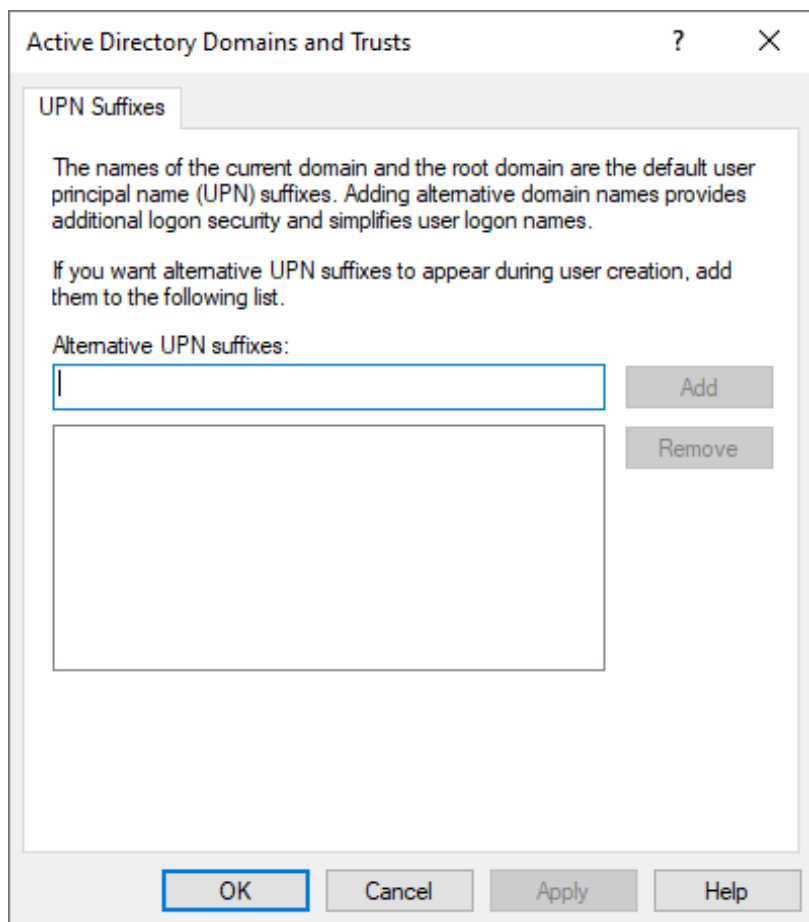
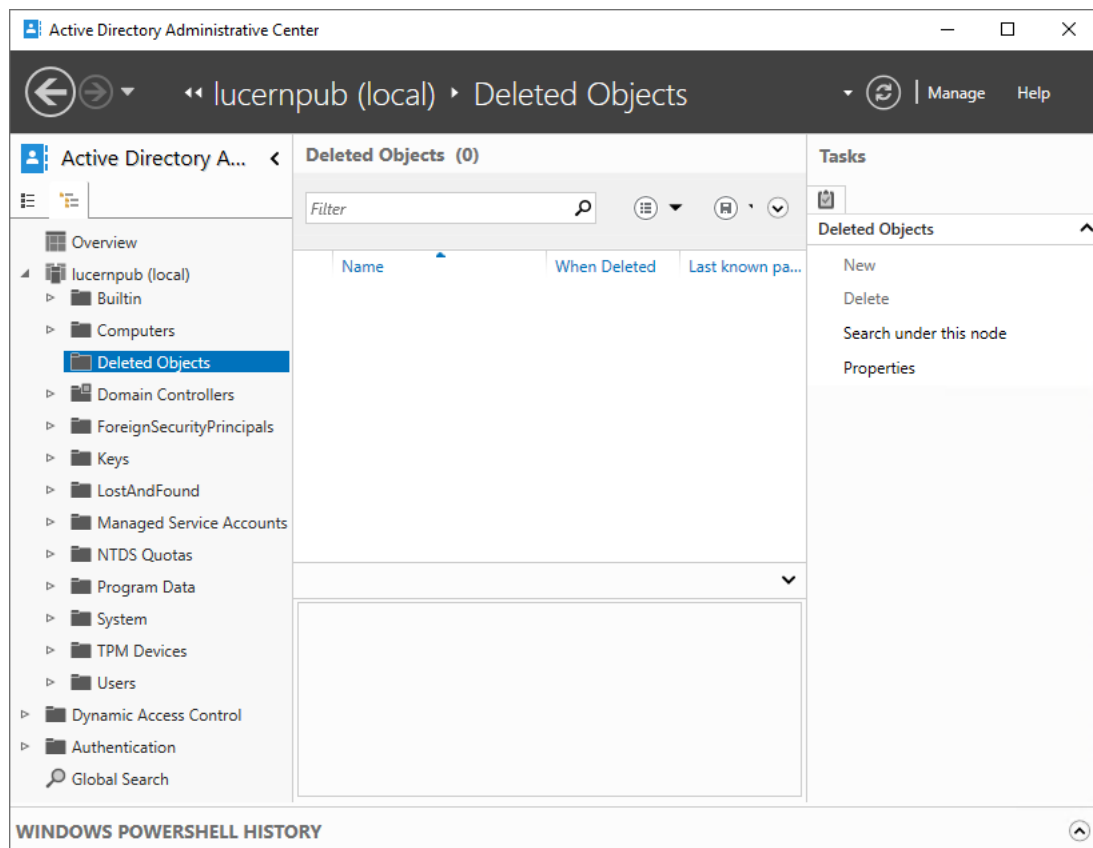
Active Directory Administrative Center



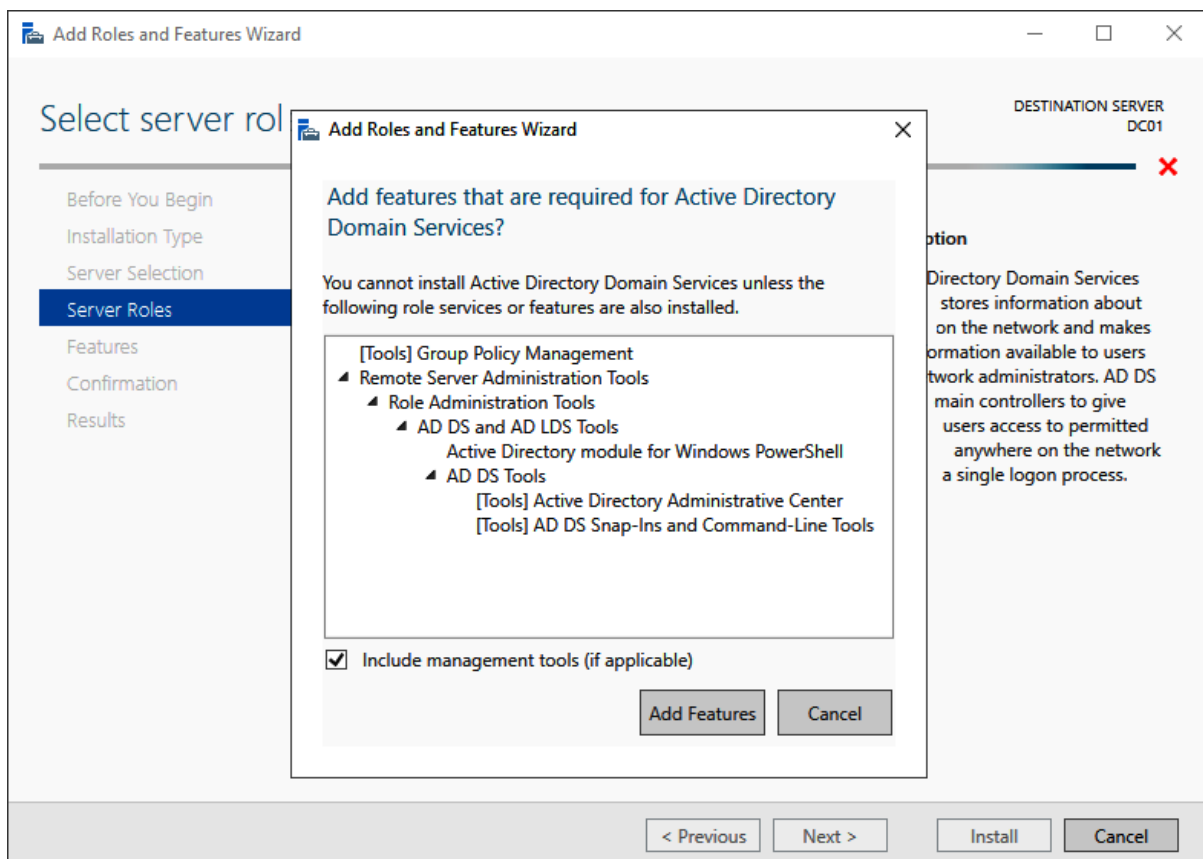
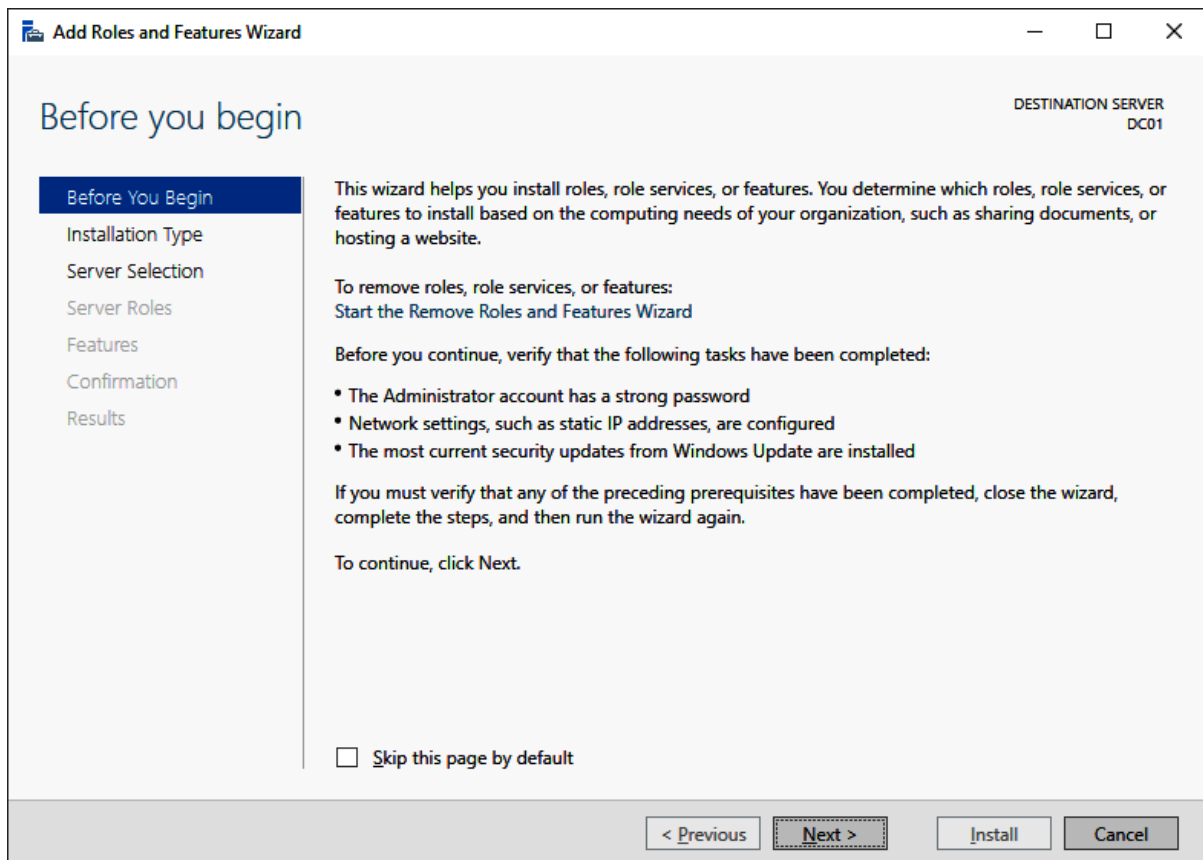
Please refresh AD Administrative Center now.

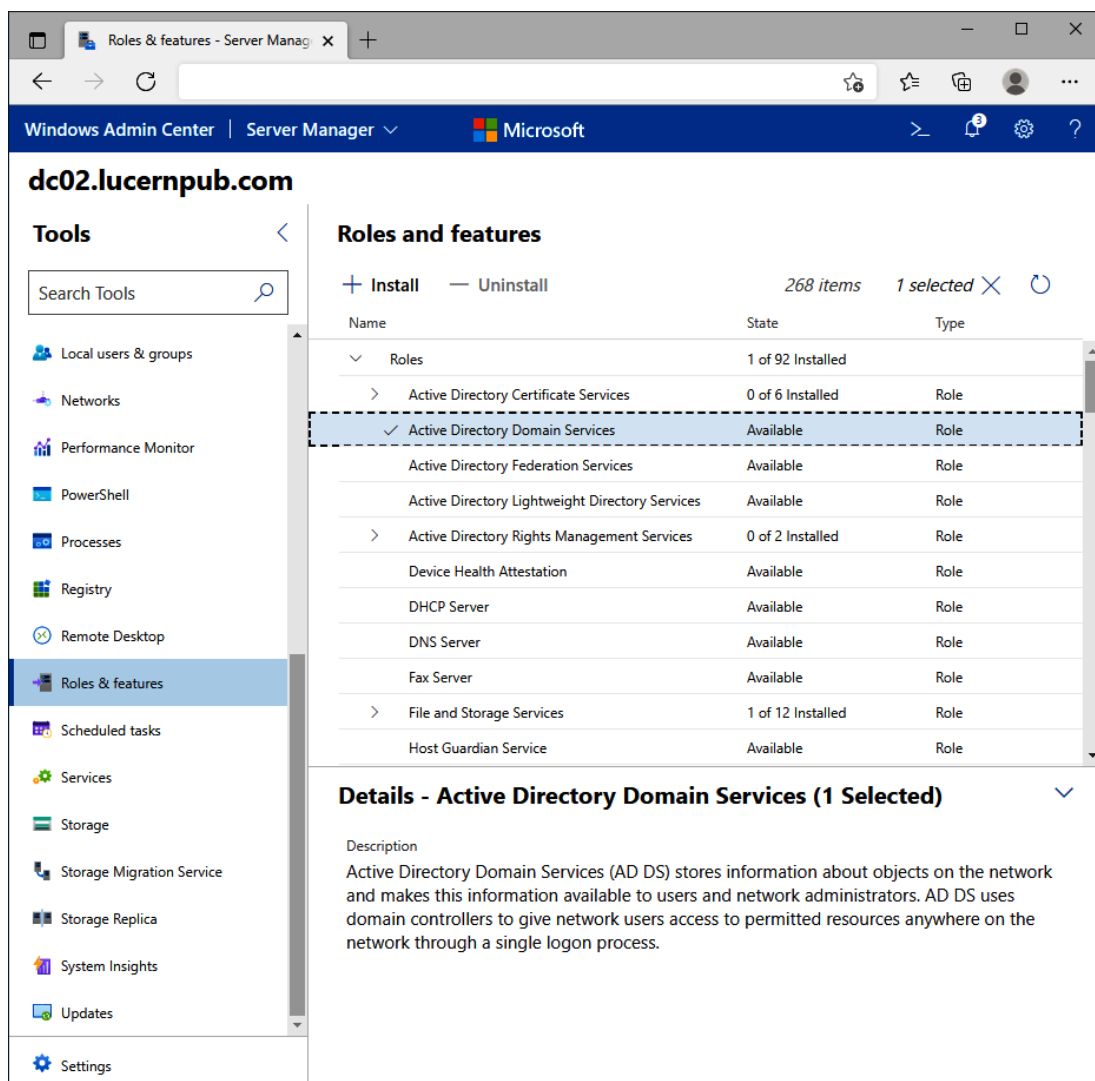
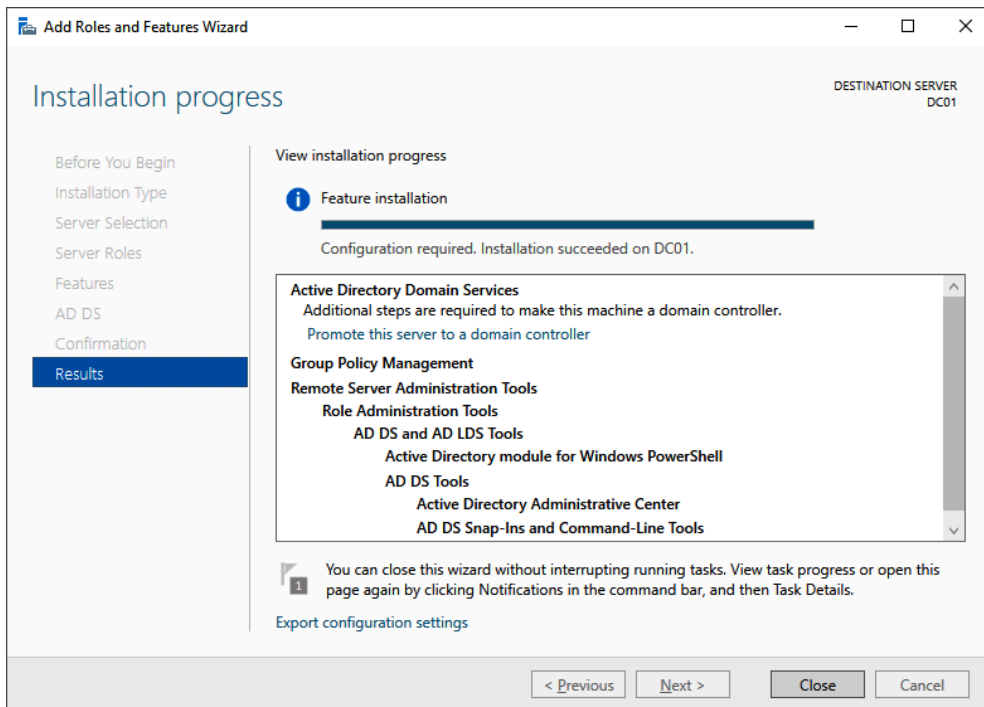
AD DS has begun enabling Recycle Bin for this forest. The Recycle Bin will not function reliably until all domain controllers in the forest have replicated the Recycle Bin configuration change.

OK



Chapter 2: Managing Domain Controllers





All Servers Task Details

All Servers Task Details and Notifications

All Tasks | 1 total

Filter

Status	Task Name	Stage	Message	Action	Notifications
	Post-deployment Configuration	Not Sta...	Configuration required for Active Directory Do...	Promote this server to a domain...	1

Status	Notification	Time Stamp
	Additional steps are required to make this machine a domain controller.	

Active Directory Domain Services Configuration Wizard

Deployment Configuration

TARGET SERVER
DC01

Deployment Configuration

Domain Controller Options

Additional Options

Paths

Review Options

Prerequisites Check

Installation

Results

Select the deployment operation

☒ Add a domain controller to an existing domain

☐ Add a new domain to an existing forest

☐ Add a new forest

Specify the domain information for this operation

Domain:

*

Select...

Supply the credentials to perform this operation

<No credentials provided>

Change...

[More about deployment configurations](#)

< Previous

Next >

Install

Cancel

Active Directory Domain Services Configuration Wizard

TARGET SERVER
DC01

Review Options

Deployment Configuration

Domain Controller Options

DNS Options

Additional Options

Paths

Review Options

Prerequisites Check

Installation

Results

Review your selections:

Configure this server as the first Active Directory domain controller in a new forest.

The new domain name is "lucernpub.com". This is also the name of the new forest.

The NetBIOS name of the domain: LUCERNPUB

Forest Functional Level: Windows Server 2016

Domain Functional Level: Windows Server 2016

Additional Options:

Global catalog: Yes

DNS Server: Yes

Create DNS Delegation: No

These settings can be exported to a Windows PowerShell script to automate additional installations

View script

More about installation options

< PreviousNext >InstallCancel

Add Roles and Features Wizard

DESTINATION SERVER
DC02

Active Directory Domain Services

Before You Begin

Installation Type

Server Selection

Server Roles

Features

AD DS


Confirmation

Results

Active Directory Domain Services (AD DS) stores information about users, computers, and other devices on the network. AD DS helps administrators securely manage this information and facilitates resource sharing and collaboration between users.

Things to note:

- To help ensure that users can still log on to the network in the case of a server outage, install a minimum of two domain controllers for a domain.
- AD DS requires a DNS server to be installed on the network. If you do not have a DNS server installed, you will be prompted to install the DNS Server role on this machine.



Azure Active Directory, a separate online service, can provide simplified identity and access management, security reporting, single sign-on to cloud and on-premises web apps.
[Learn more about Azure Active Directory](#)
[Configure Office 365 with Azure Active Directory Connect](#)

< PreviousNext >InstallCancel

Active Directory Domain Services Configuration Wizard

Domain Controller Options

TARGET SERVER
DC02

Deployment Configuration

Domain Controller Options

RODC Options

Additional Options

Paths

Review Options

Prerequisites Check

Installation

Results

Specify domain controller capabilities and site information

☒ Domain Name System (DNS) server

☒ Global Catalog (GC)

☒ Read only domain controller (RODC)

Site name:

Default-First-Site-Name

Type the Directory Services Restore Mode (DSRM) password

Password: *

Confirm password: *

[More about domain controller options](#)

< Previous

Next >

Install

Cancel

Active Directory Domain Services Configuration Wizard

RODC Options

TARGET SERVER
DC02

Deployment Configuration

Domain Controller Options

RODC Options

Additional Options

Paths

Review Options

Prerequisites Check

Installation

Results

Delegated administrator account

<Not provided>

Select...

Accounts that are allowed to replicate passwords to the RODC

LUCERNPUB\Allowed RODC Password Replication Group

Add...

Remove

Accounts that are denied from replicating passwords to the RODC

BUILTIN\Administrators

BUILTIN\Server Operators

BUILTIN\Backup Operators

Add...

Remove

If the same account is both allowed and denied, denied takes precedence.

[More about RODC options](#)

< Previous

Next >

Install

Cancel

Active Directory Domain Services Configuration Wizard

TARGET SERVER
DC02

Paths

Deployment Configuration
Domain Controller Options
RODC Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results

Specify the location of the AD DS database, log files, and SYSVOL

Database folder: C:\Windows\NTDS

Log files folder: C:\Windows\NTDS

SYSVOL folder: C:\Windows\SYSVOL

[More about Active Directory paths](#)

< Previous Next > Install Cancel

Active Directory Domain Services Configuration Wizard

TARGET SERVER
DC02

Additional Options

Deployment Configuration
Domain Controller Options
RODC Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results

Specify Install From Media (IFM) Options

☐ Install from media

Specify additional replication options

Replicate from: Any domain controller

[More about additional options](#)

< Previous Next > Install Cancel

DefaultDCCloneAllowList - Notepad

```
File Edit Format View Help
<DefaultCloneConfig>
  <AllowList>
    <!-- Service types -->
    <Allow>
      <Name>ADWS</Name>
      <Type>Service</Type>
    </Allow>
    <Allow>
      <Name>AeLookupSvc</Name>
      <Type>Service</Type>
    </Allow>
    <Allow>
      <Name>ALG</Name>
      <Type>Service</Type>
    </Allow>
    <Allow>
      <Name>AllUserInstallAgent</Name>
      <Type>Service</Type>
    </Allow>
    <Allow>
      <Name>AppIDSvc</Name>
      <Type>Service</Type>
    </Allow>
    <Allow>
      <Name>Appinfo</Name>
      <Type>Service</Type>
    </Allow>
    <Allow>
      <Name>AppMgmt</Name>
    </Allow>
```

Ln 1, Col 1 100% Windows (CRLF) UTF-8

Remove Roles and Features Wizard

Remove server

Before You Begin
Server Selection
Server Roles
Features
Confirmation
Results

DESTINATION SERVER
DC03.lucernpub.com

Remove Roles and Features Wizard

Remove features that require Active Directory Domain Services?

You can remove management tools, or leave them installed on this server to manage other servers.

- [Tools] Group Policy Management
 - Remote Server Administration Tools
 - Role Administration Tools
 - AD DS and AD LDS Tools
 - AD DS Tools
 - Active Directory Administrative Center
 - [Tools] AD DS Snap-Ins and Command-Line Tools

☒ Remove management tools (if applicable)

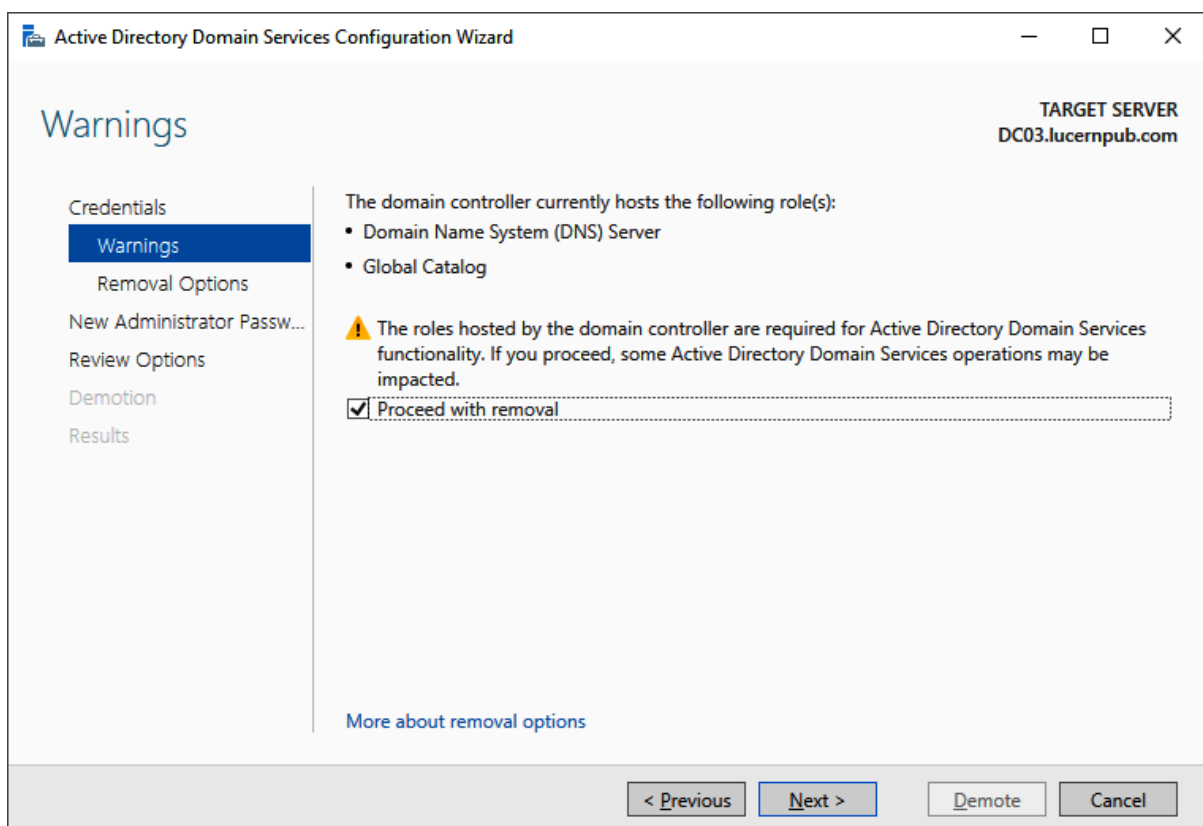
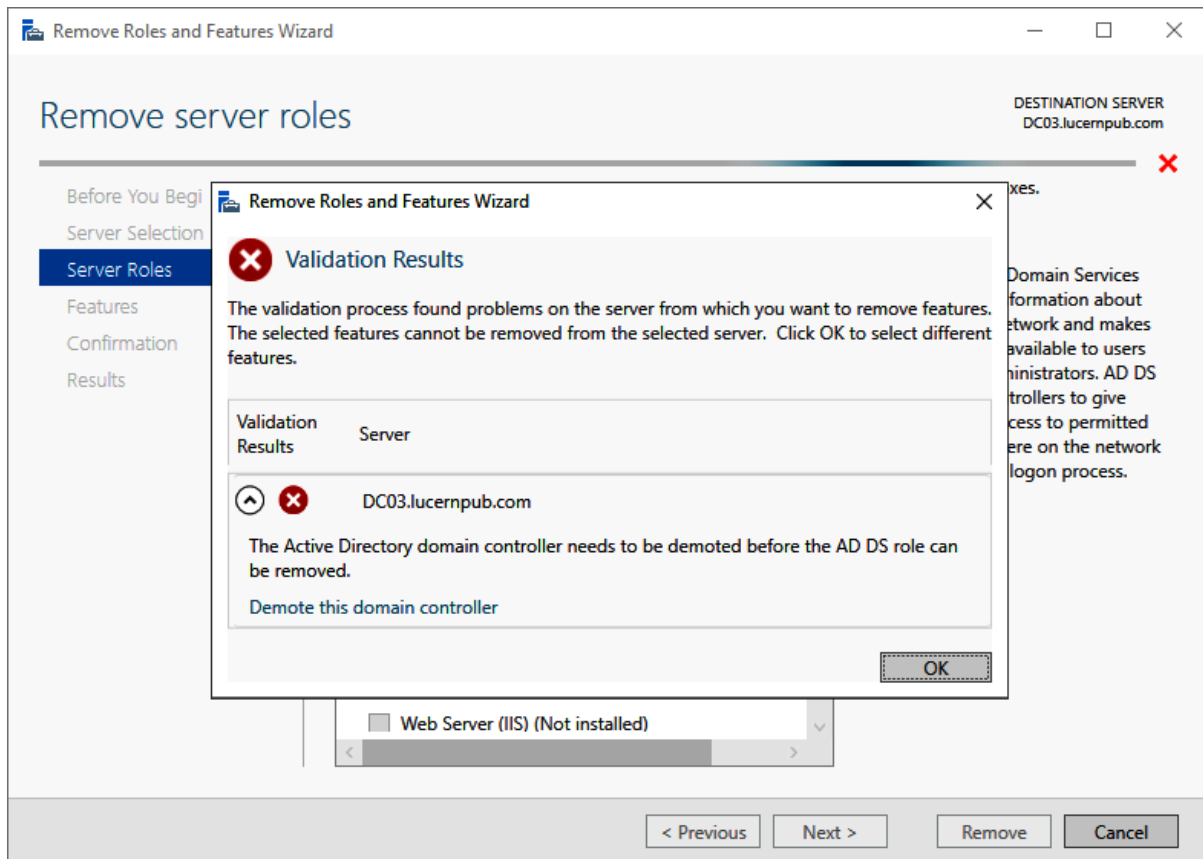
Remove Features Cancel

< Previous Next > Remove Cancel

check boxes.

option

Directory Domain Services stores information about on the network and makes information available to users network administrators. AD DS main controllers to give users access to permitted es anywhere on the network a single logon process.



Active Directory Domain Services Configuration Wizard

Credentials

Warnings

Removal Options

New Administrator Passw...

Review Options

Demotion

Results

TARGET SERVER
DC03.lucernpub.com

Supply the credentials to perform this operation

LUCERNPUB\adminsanderb (Current user)

☐ Force the removal of this domain controller

Change...

The server will be automatically restarted after the demotion operation. Role removal needs to be performed after the restart.

More about removal credentials

< Previous

Next >

Demote

Cancel

Active Directory Administrative Center

Active Directory Administrative Center > Overview

Manage Help

Active Directory... <

CONTENT

Overview

lucernpub (local)

Domain Controllers

Dynamic Access Control

Authentication

Global Search

WELCOME TO ACTIVE DIRECTORY ADMINISTRATIVE CENTER

LEARN MORE

DYNAMIC ACCESS CONTROL

AZURE ACTIVE DIRECTORY

Learn more about Active Directory Administrative Center

Use Active Directory Administrative Center to manage IT tasks

Use Active Directory module for Windows PowerShell

Find answers on Active Directory Forum

Deploy Dynamic Access Control

Get Microsoft Solution Accelerator to help configure Dynamic Access

Deploy Authentication Policies and Silos

RESET PASSWORD

User name: Domain\UserName

Password:

Confirm password:

☒ User must change password at next log on

☐ Unlock account

Apply Clear

GLOBAL SEARCH

DC04

Scope: lucernpub (local)

WINDOWS POWERSHELL HISTORY

Active Directory Administrative Center

Domain System Volume > Topology >

Active Directory... < Topology (2)

Filter

Name	Type	Description
DC01	msDFS-M...	
DC04	msDFS-M...	

DC04

Object class: msDFS-Member Modified: 10/3/2021 6:58 PM

Description:

Summary

Tasks

DC04

- New
- Delete
- Move...
- Search under this node
- Properties

Topology

- New
- Delete
- Move...
- Search under this node
- Properties

WINDOWS POWERSHELL HISTORY

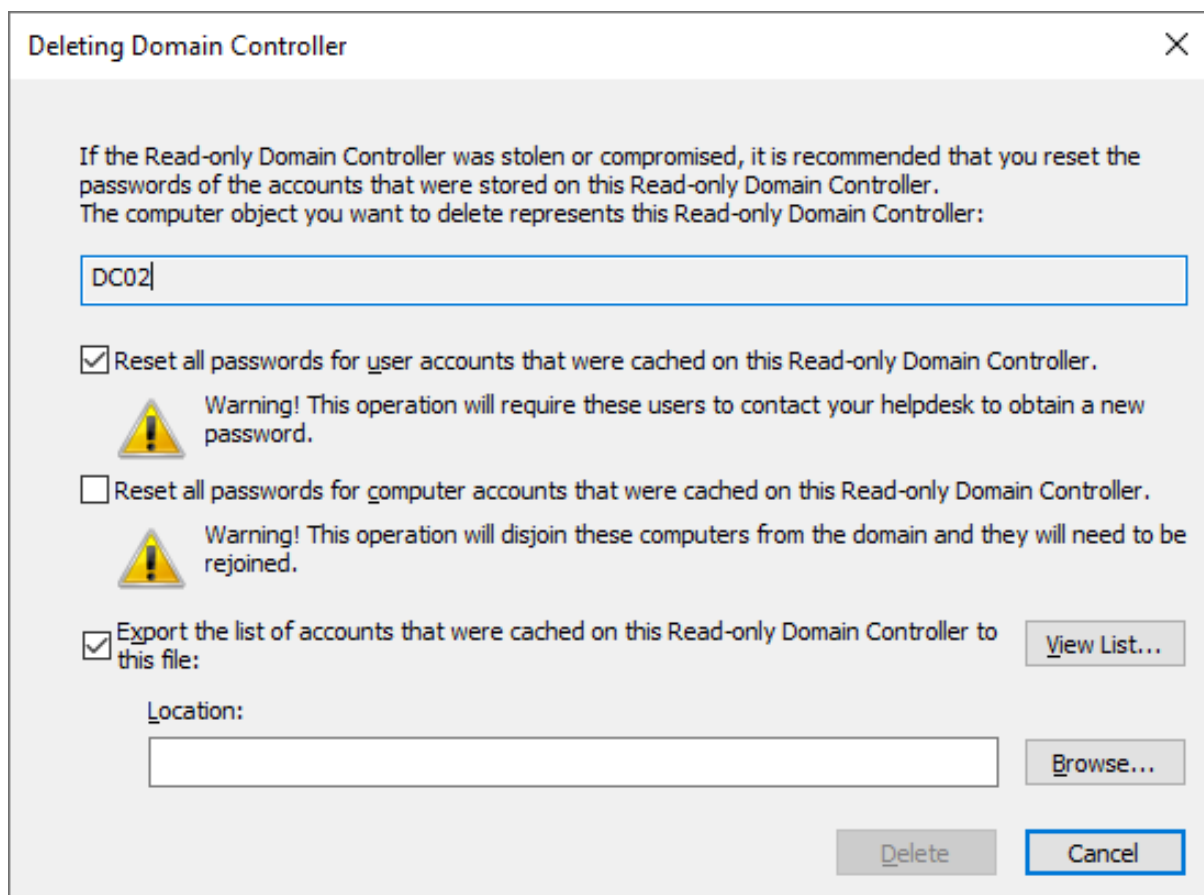
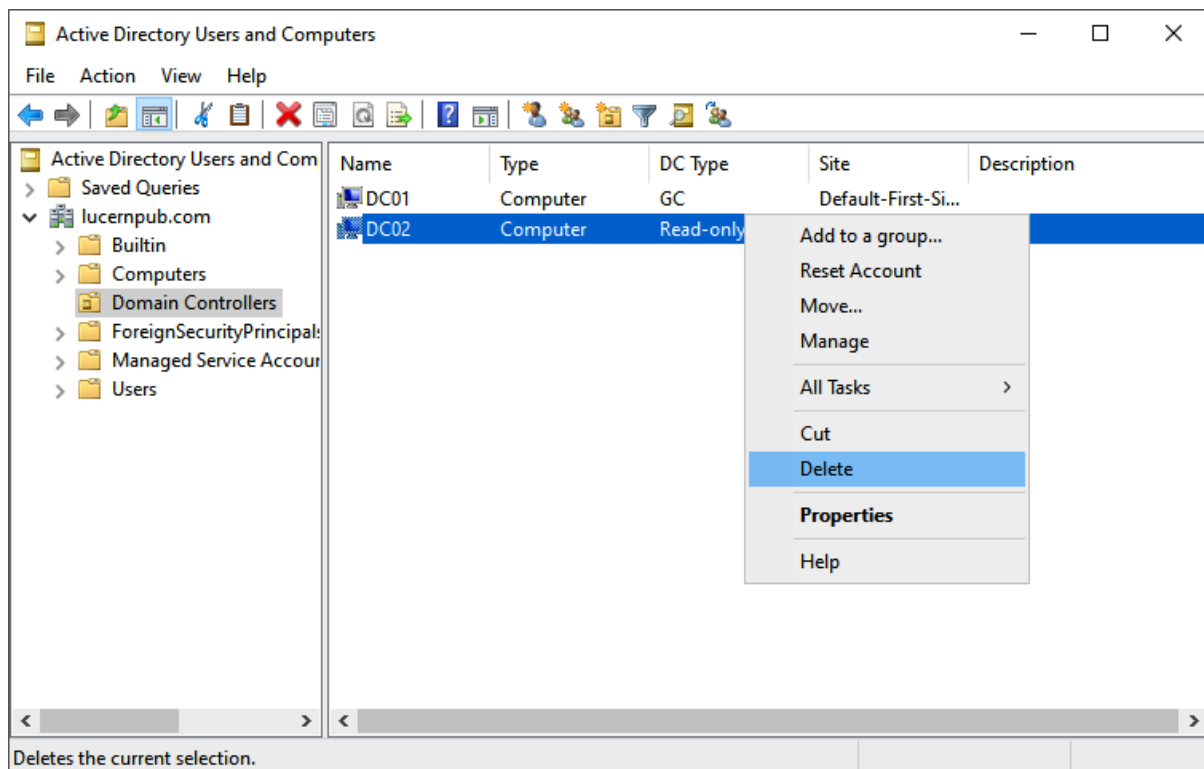
Active Directory Sites and Services

File Action View Help

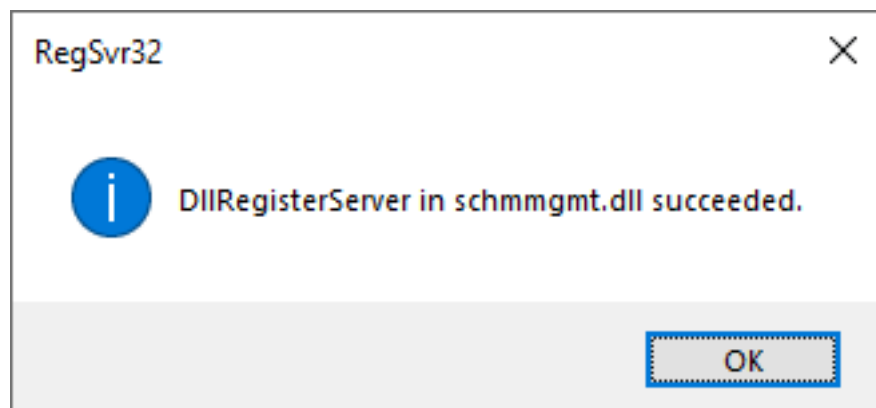
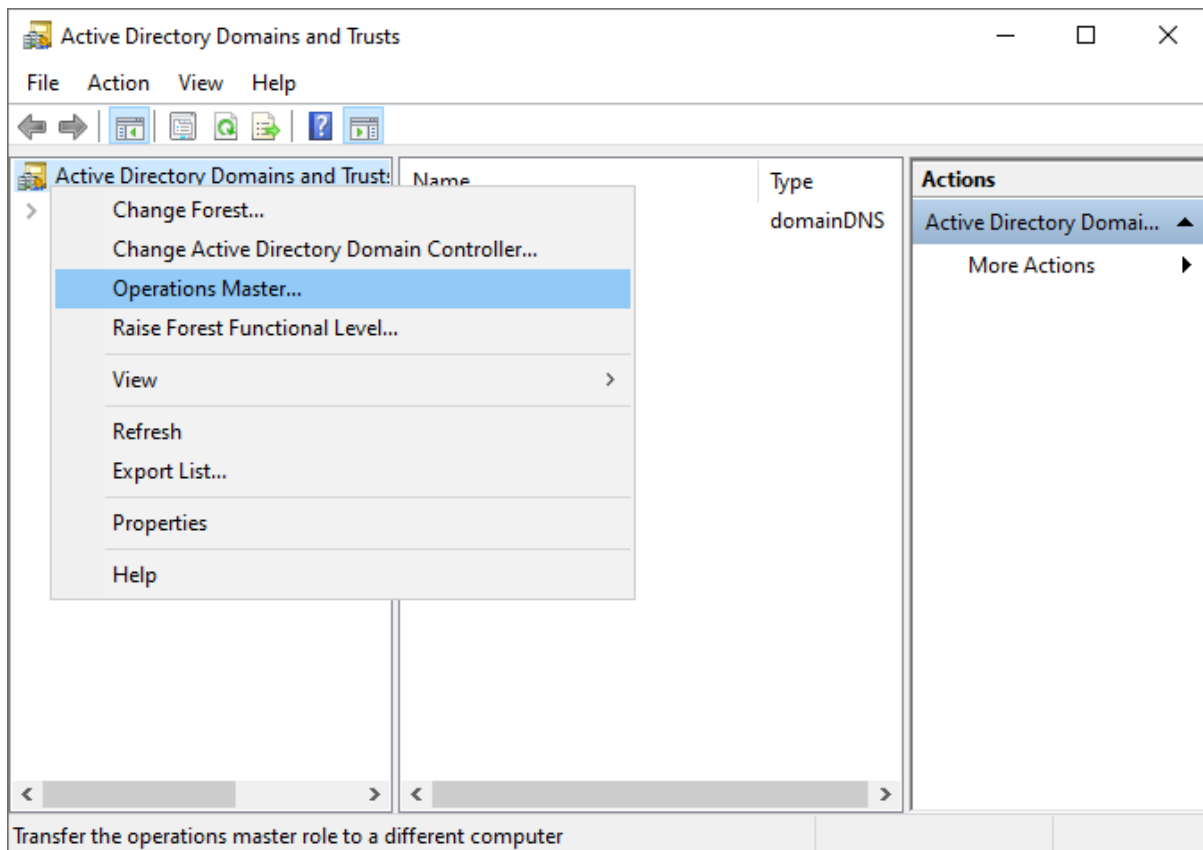
Active Directory Sites and Services

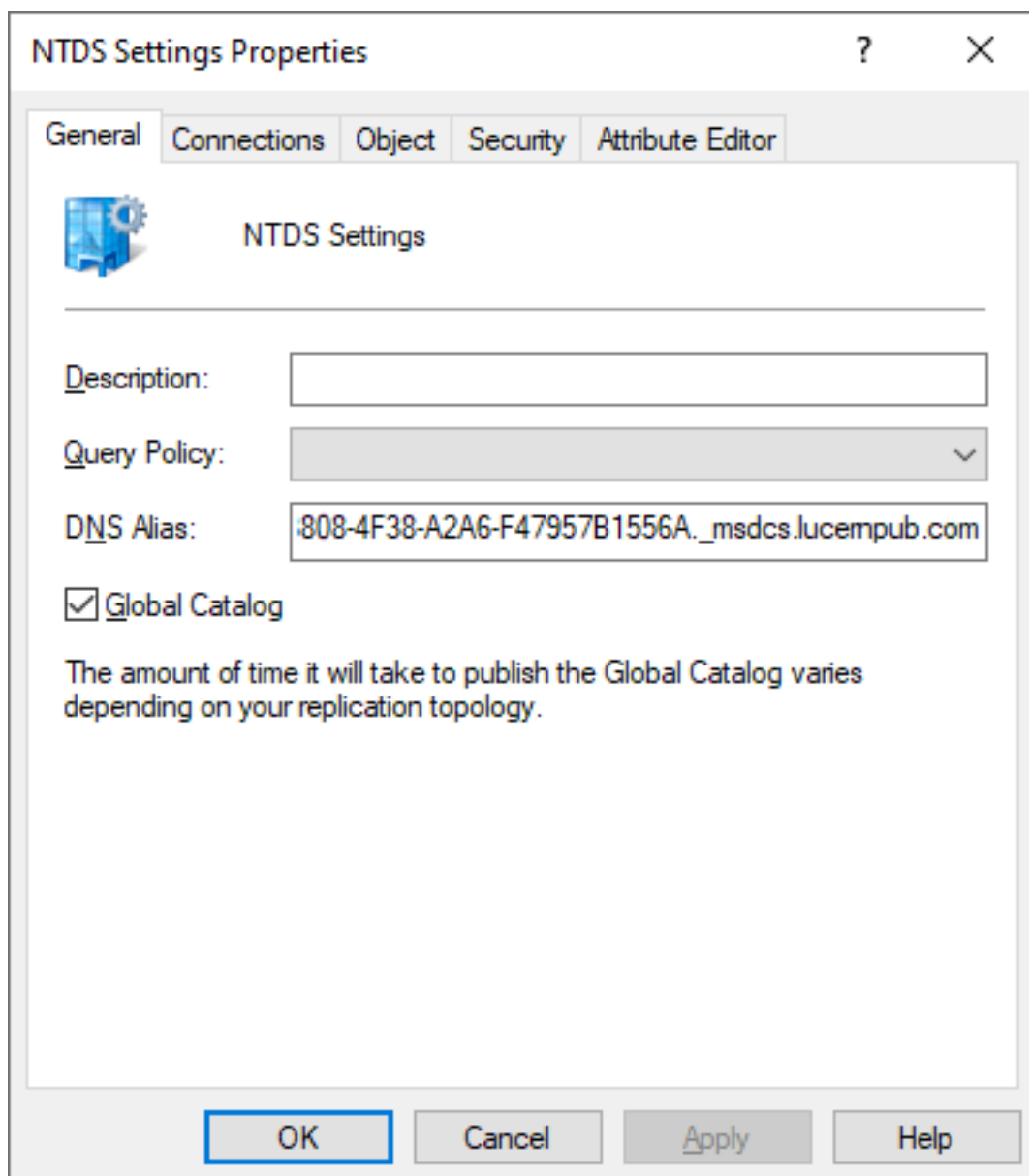
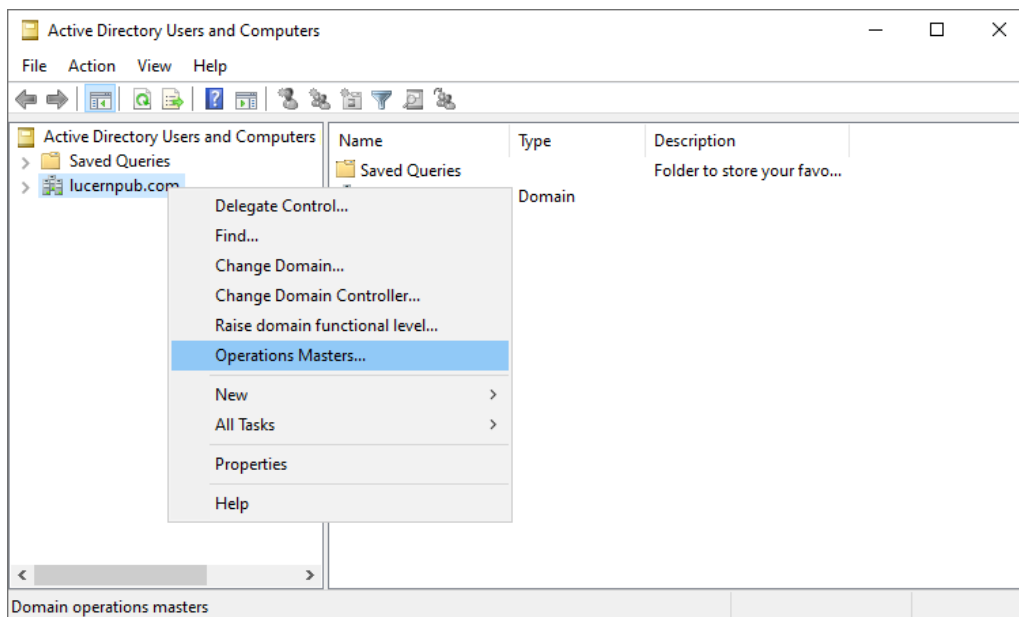
Sites

Name	Type	Description
Sites	Sites Container	

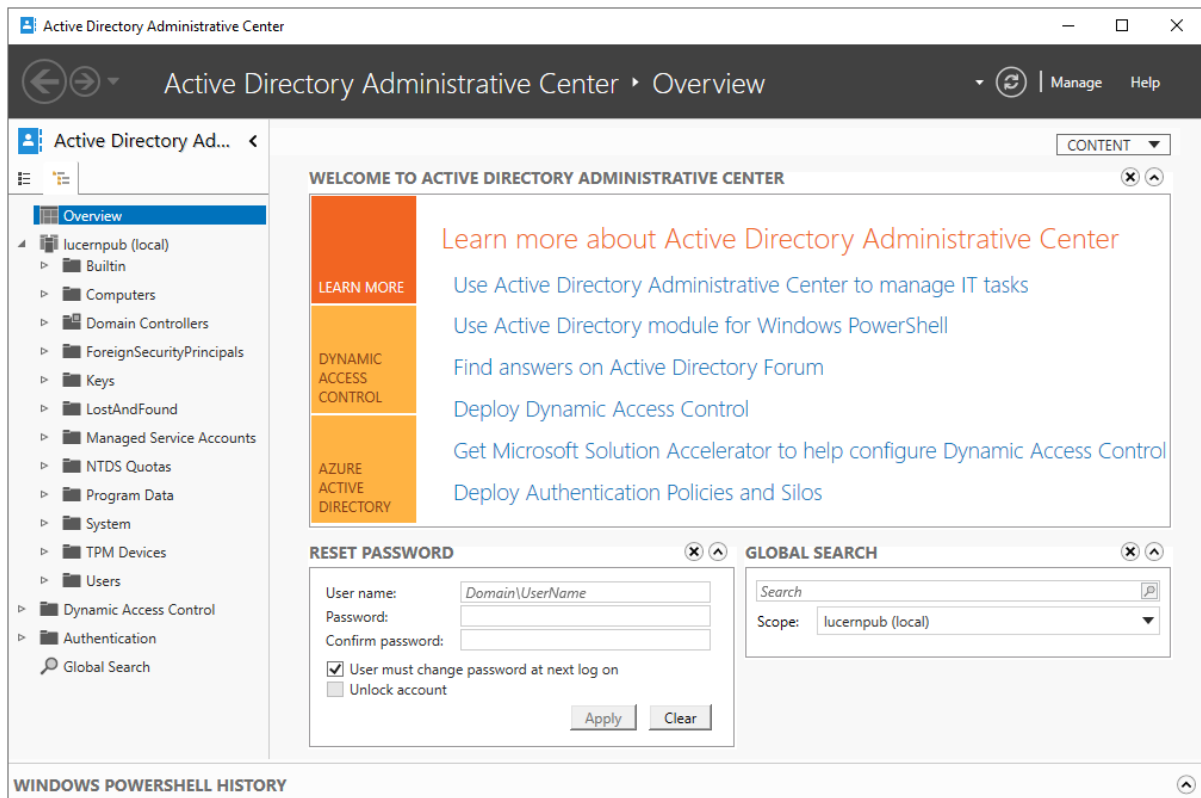


Chapter 3: Managing Active Directory Roles and Features





Chapter 4: Managing Containers and Organizational Units



Create Organizational Unit: TASKS ▼ SECTIONS ▼

*** Organizational Unit**

Managed By

Organizational Unit ? ✕ ⬆

Name: *

Create in: DC=lucernpub,DC=com [Change...](#)

Address:

Description:

☐ Protect from accidental deletion

City State/Province Zip/Postal code

Country/Region:

Managed By ? ✕ ⬆

Managed by: [Edit...](#) [Clear](#) Office:

Phone numbers:

Main:

Mobile:

Fax:


Address:

City State/Province Zip/Postal code

Country/Region:

[More Information](#) OK Cancel

Delete Confirmation



Are you sure you want to delete the Organizational Unit
Organizational Unit?

Yes

No

Organizational Unit

TASKSSECTIONSD

Organizational Unit

Managed By

Extensions

Organizational Unit

Name:

*

Organizational Unit

Description:

This is an organizational unit.

Address:

Street

City

State/Province

Zip/Postal code

Country/Region:

☒ Protect from accidental deletion

Managed By

Managed by:

Edit...Clear

Office:

Phone numbers:

Main:Mobile:Fax:

Address:

Street

City

State/Province

Zip/Postal code

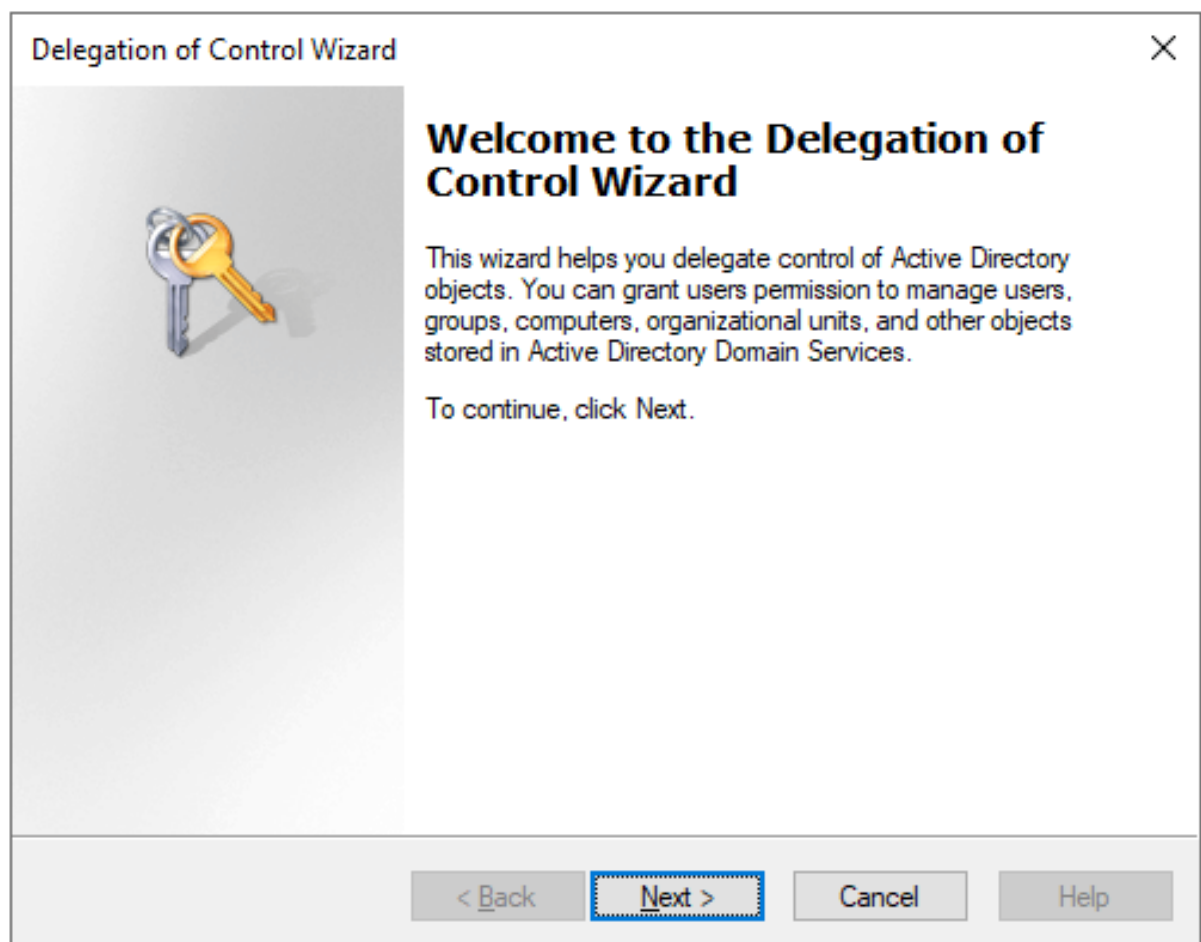
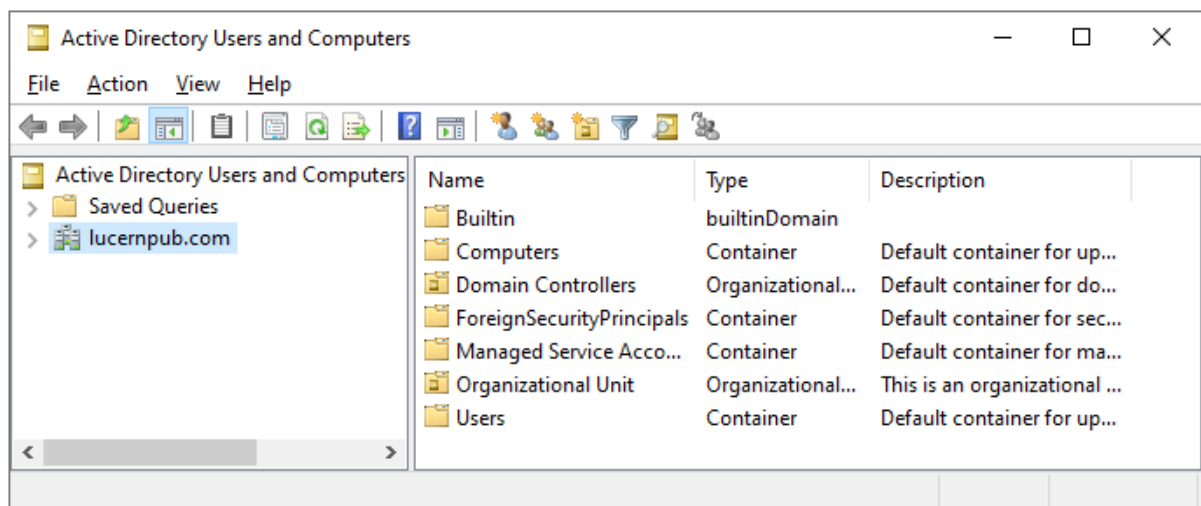
Country/Region:

Extensions

COM+SecurityAttribute Editor

More Information

OKCancel



Delegation of Control Wizard



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)

☐ Create a custom task to delegate

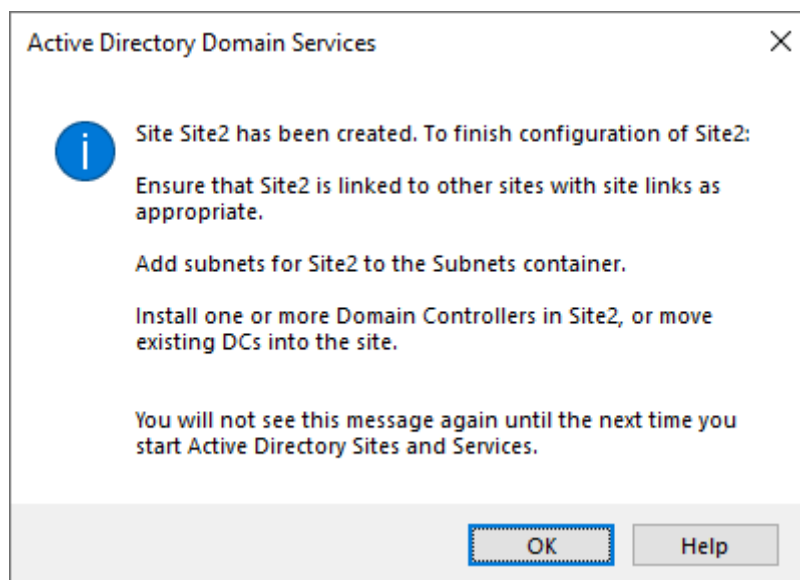
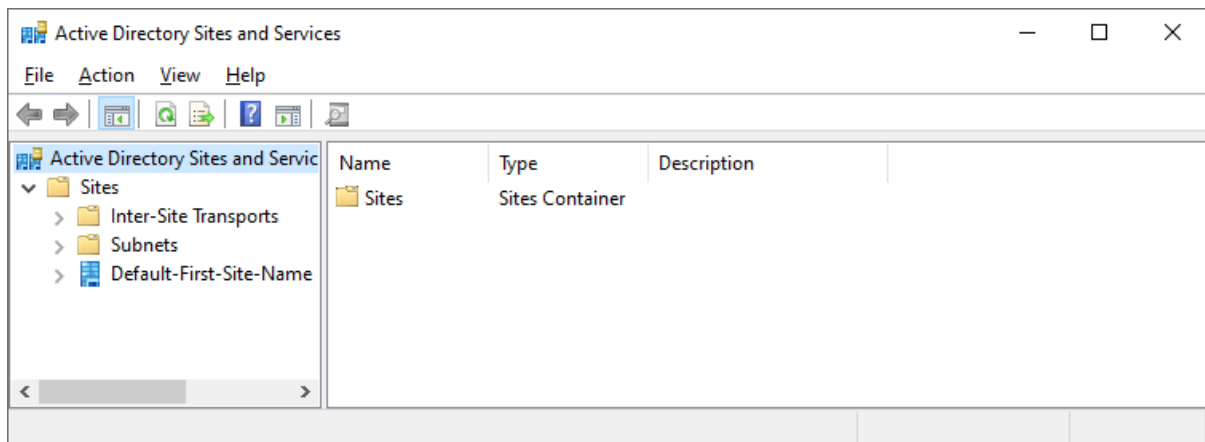
< Back

Next >

Cancel

Help

Chapter 5: Managing Active Directory Sites and Troubleshooting Replication



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.

< Back

Next >


Cancel

Help

Delegation of Control Wizard

Tasks to Delegate

You can select common tasks or customize your own.



☒ Delegate the following common tasks

☐ Manage Group Policy links

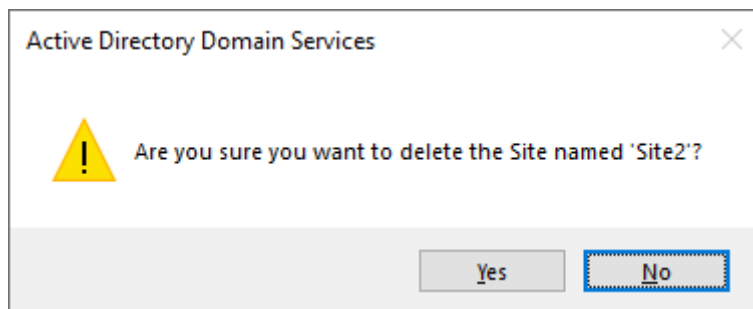
☐ Create a custom task to delegate

< Back

Next >

Cancel

Help



New Object - Subnet

Create in: lucempub.com/Configuration/Sites/Subnets

Enter the address prefix using network prefix notation (address/prefix length), where the prefix length indicates the number of fixed bits. You can enter either an IPv4 or an IPv6 subnet prefix.
[Learn more about entering address prefixes.](#)


IPv4 example: 157.54.208.0/20
IPv6 example: 3FFE:FFFF:0:C000::/64

Prefix:

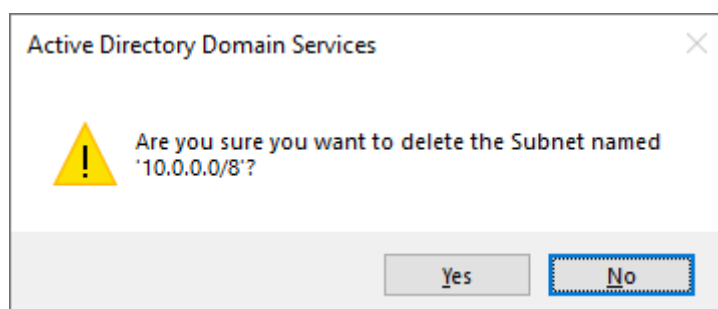
Prefix name in Active Directory Domain Services:

Select a site object for this prefix.


Site Name

 Default-First-Site-Name

OK Cancel Help



New Object - Site Link



Create in: lucempub.com/Configuration/Sites/Inter-Site

Name:

Sites not in this site link:

Site1
Site2
Site3

Add >>

<< Remove


Sites in this site link:

A site link must contain at least two sites.

OK

Cancel

Active Directory Domain Services



Are you sure you want to delete the Site Link named 'Site Link'?

Yes

No

Chapter 6: Managing Active Directory Users

Create User: TASKS SECTIONS

* Account

Organization

Member Of

Password Settings

Profile

Policy

Silo

Account

First name:

Middle initials:

Last name:

Full name: *

User UPN logon: @

User SamAccountName: *

Password:

Confirm password:

Create in: [Change...](#)

☐ Protect from accidental deletion

[Log on hours...](#) [Log on to...](#)

Account expires: ☒ Never ☐ End of

Password options:

☒ User must change password at next log on

☐ Other password options

☐ Microsoft Passport or smart card is required

☐ Password never expires

☐ User cannot change password

Encryption options:

Other options:

Organization

Display name:

Office:

E-mail:

Web page:

Job title:

Department:

Company:

Manager:

[Edit...](#) [Clear](#)

[More Information](#) OK Cancel

Find Users, Contacts, and Groups

File Edit View

Find: Users, Contacts, and Groups In: Browse...

Users, Contacts, and Groups Advanced

Name:

Description:

[Find Now](#)

[Stop](#)

[Clear All](#)

Search results:

Name	Type	Description
Users	Group	Users are prevented from making a
User	User	

2 item(s) found

User Properties

Security	Environment	Sessions	Remote control		
Remote Desktop Services Profile			COM+		
General	Address	Account	Profile	Telephones	Organization
Published Certificates	Member Of	Password Replication	Dial-in	Object	

Canonical name of object:

Object class: User

Created: 11/29/2021 8:04:18 AM

Modified: 11/29/2021 8:04:18 AM

Update Sequence Numbers (USNs):


Current: 20517

Original: 20512

☒ Protect object from accidental deletion

OK Cancel Apply Help

Active Directory Domain Services

 Are you sure you want to delete the user named 'User'?

Yes No

User

TASKS

SECTIONS

Account

Organization

Member Of

Password Settings

Profile

Policy

Silo

Extensions

Account

First name:

Middle initials:

Last name:

Full name: *

User UPN login: user @

User SamAccoun... * user

☒ Protect from accidental deletion

Log on hours...

Log on to...

Account expires: ☒ Never ☐ End of

Password options: ☒ User must change password at next log on ☐ Other password options

☐ Microsoft Passport or smart card is requ...

☐ Password never expires

☐ User cannot change password

Encryption options:

Other options:

Organization

Display name:

Office:

E-mail:

Web page:

Job title:

Department:

Company:

Manager: Edit... Clear

Direct reports: Add...

Phone numbers:


Other web pages...

More Information

OK

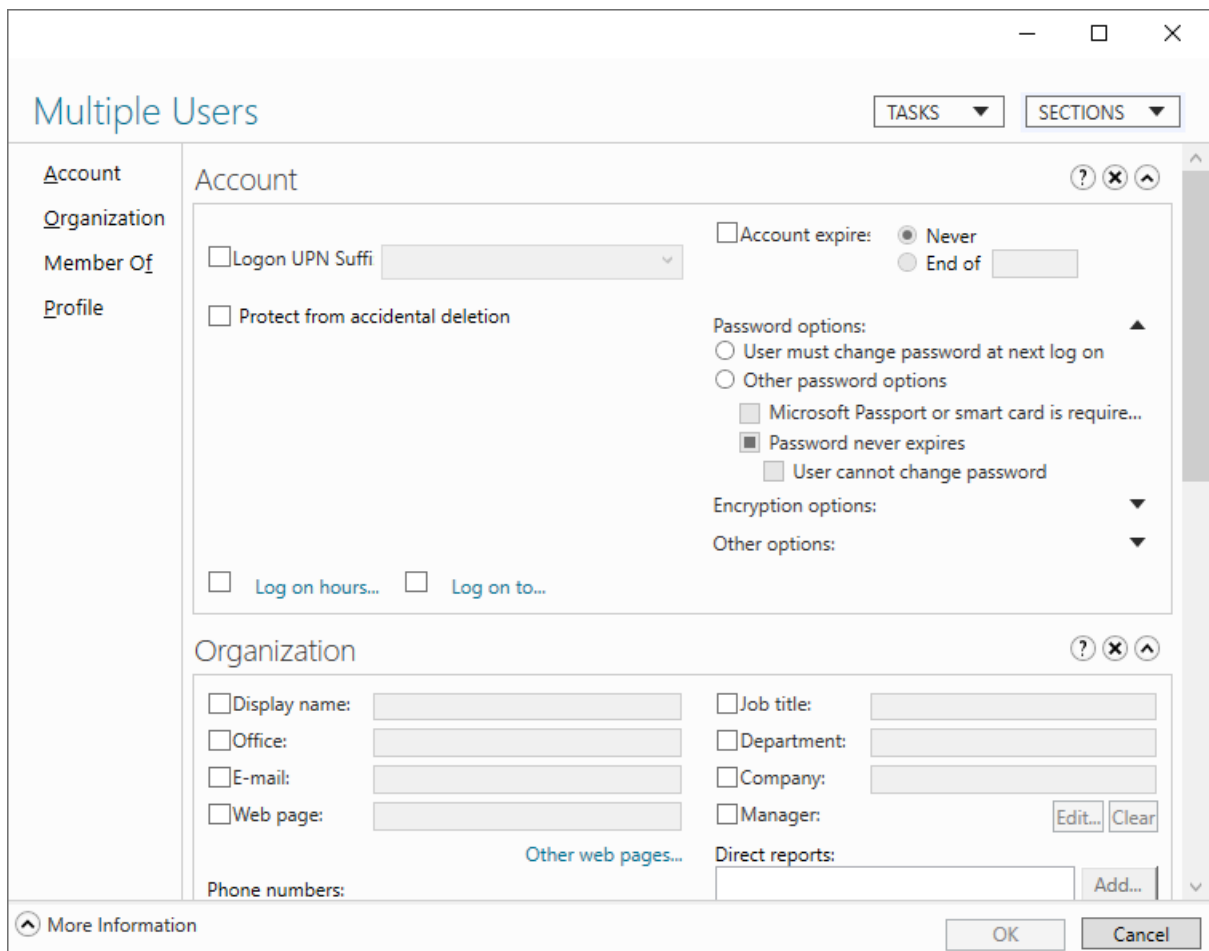
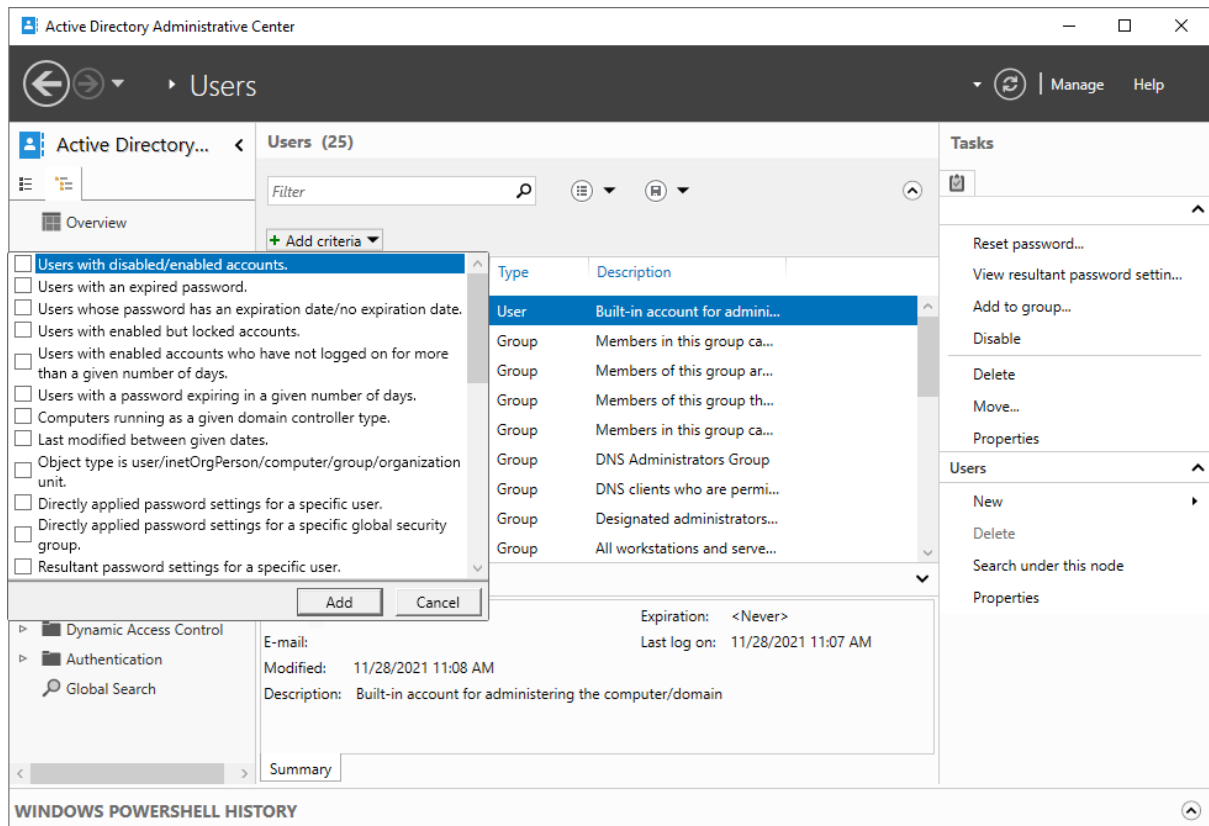
Cancel

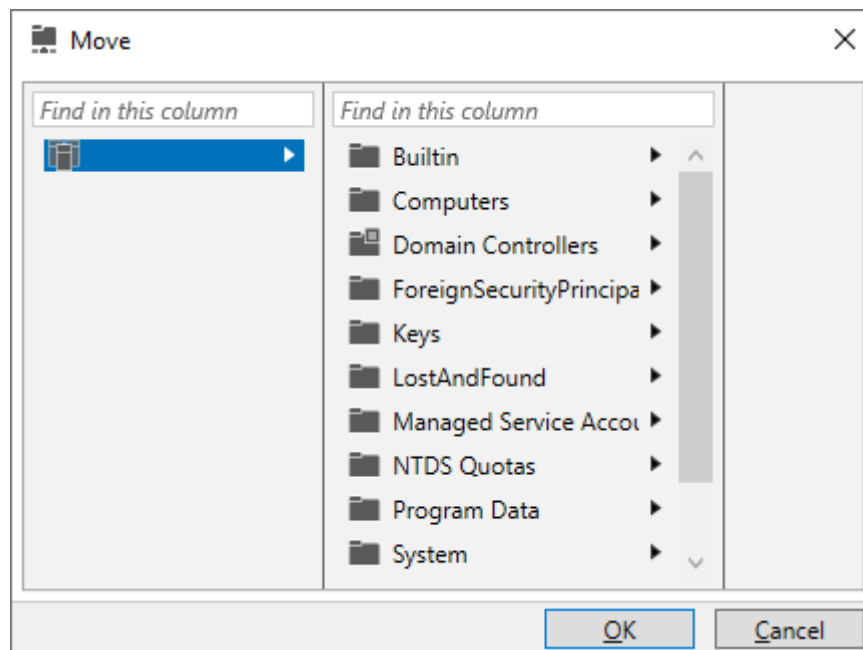
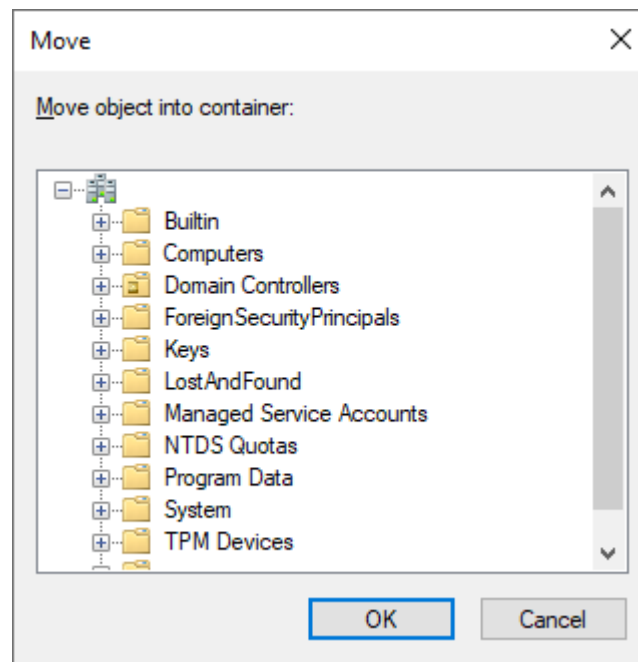
Delete Confirmation

 Are you sure you want to delete the User User?

Yes

No





Rename User ? X

Full name:

First name:

Last name:

Display name:

User logon name:

User logon name (pre-Windows 2000):

OK Cancel

User TASKS SECTIONS

Account Organization Member Of Password Settings Profile Policy Silo Extensions

Account

First name:

Middle initials:

Last name:

Full name: *

User UPN logon: @

User SamAccountName: *

☐ Protect from accidental deletion

Log on hours... Log on to...

Organization

Display name:

Office:

E-mail:

Web page:

Other web pages...

Job title:

Department:

Company:

Manager: Edit... Clear

Direct reports: Add...

Phone numbers:

More Information

OK Cancel

Context Menu:

- Delete
- Move...
- Disable
- Reset password...
- Help

Password options:

- ☒ User must change password at next log on
- ☐ Other password options
 - ☐ Microsoft Passport or smart card is requ...
 - ☐ Password never expires
 - ☐ User cannot change password

Encryption options:

Other options:

Active Directory Administrative Center

Users

ManageHelp

Active Directory... < Users (25)

Filter

+ Add criteria

Overview

☐ Users with disabled/enabled accounts.

☐ Users with an expired password.

☐ Users whose password has an expiration date/no expiration date.

☒ Users with enabled but locked accounts.

☐ Users with enabled accounts who have not logged on for more than a given number of days.

☐ Users with a password expiring in a given number of days.

☐ Computers running as a given domain controller type.

☐ Last modified between given dates.

☐ Object type is user/inetOrgPerson/computer/group/organization unit.

☐ Directly applied password settings for a specific user.

☐ Directly applied password settings for a specific global security group.

☐ Resultant password settings for a specific user.

AddCancel

TypeDescription

UserBuilt-in account for admini...

GroupMembers in this group ca...

GroupMembers of this group ar...

GroupMembers of this group th...

GroupMembers in this group ca...

GroupDNS Administrators Group

GroupDNS clients who are permi...

GroupDesignated administrators...

GroupAll workstations and serve...

Expiration: <Never>

Last log on: 11/28/2021 11:07 AM

E-mail:

Modified: 11/28/2021 11:08 AM

Description: Built-in account for administering the computer/domain

Summary

Tasks

Reset password...

View resultant password settin...

Add to group...

Disable

Delete

Move...

Properties

Users

New

Delete

Search under this node

Properties

WINDOWS POWERSHELL HISTORY

User

TASKSSECTIONSD

Account

Organization

Member Of

Password Settings

Profile

Policy

Silo

Extensions

Account

First name:

Middle initials:

Last name:

Full name: * User

User UPN logon: user @

User SamAccoun... * user

☐ Protect from accidental deletion

Log on hours... Log on to... Unlock account

Account expires: ☒ Never ☐ End of

Password options:

Encryption options:

Other options:

Organization

Display name:

Office:

E-mail:

Web page:

Phone numbers: Main: Home: Mobile:

Job title:

Department:

Company:

Manager: Edit... Clear

Direct reports: Add... Remove

Other web pages...

More Information

OKCancel

User Properties ? X

Published Certificates	Member Of	Password Replication	Dial-in	Object
Security	Environment	Sessions	Remote control	
General	Address	Account	Profile	Telephones
Remote Desktop Services Profile	COM+	Attribute Editor		

Attributes:

Attribute	Value
uid	<not set>
uidNumber	<not set>
unicodePwd	<not set>
unixHomeDirectory	<not set>
unixUserPassword	<not set>
url	<not set>
userAccountControl	0x200 = (NORMAL_ACCOUNT)
userCert	<not set>
userCertificate	<not set>
userParameters	<not set>
userPassword	<not set>
userPKCS12	<not set>
userPrincipalName	user@lucempub.com
userSharedFolder	<not set>

Edit Filter

OK Cancel Apply Help

User TASKS SECTIONS

Account
Organization
Member Of
Password Settings
Profile
Policy
Silo
Extensions

Extensions ? X

COM+	Environment	Sessions	Remote control
Remote Desktop Services Profile	Security	Dial-in	
Published Certificates	Password Replication	Attribute Editor	

Attributes:

Attribute	Value
thumbnailLogo	<not set>
thumbnailPhoto	<not set>
title	<not set>
uid	<not set>
uidNumber	<not set>
unicodePwd	<not set>
unixHomeDirectory	<not set>
unixUserPassword	<not set>
url	<not set>
userAccountControl	0x200 = (NORMAL_ACCOUNT)
userCert	<not set>
userCertificate	<not set>
userParameters	<not set>
userPassword	<not set>

Edit Filter

More Information OK Cancel

Attribute Editor Security

Attributes:

Attribute	Value
userAccountControl	0x200 = (NORMAL_ACCOUNT)
userCert	<not set>

Integer Attribute Editor

Attribute: userAccountControl

Value:

512

Clear OK Cancel

uSNChanged 24625
uSNCreated 20523
uSNDLastObjRem... <not set>

Edit Filter

OK Cancel Apply Help

User Properties

Published Certificates Member Of Password Replication Dial-in Object
Security Environment Sessions Remote control
Remote Desktop Services Profile COM+ Attribute Editor
General Address Account Profile Telephones Organization

User logon name:
user

User logon name (pre-Windows 2000):
user

Logon Hours... Log On To...

☐ Unlock account

Account options:

- ☐ User must change password at next logon
- ☐ User cannot change password
- ☐ Password never expires
- ☐ Store password using reversible encryption

Account expires

☐ Never ☒ End of Tuesday , December 31, 2024

OK Cancel Apply Help

User

TASKS

SECTIONS

Account

Organization

Member Of

Password Settings

Profile

Policy

Silo

Extensions

Account

First name:

Middle initials:

Last name:

Full name: *

User UPN login: user @

User SamAccountName: * user

Account expires: ☐ Never ☒ End of

Protect from accidental deletion

Log on hours...

Log on to...

Password options:

Encryption options:

Other options:

Organization

Display name:

Office:

E-mail:

Web page:

Job title:

Department:

Company:

Manager: Edit... Clear

Other web pages...

Direct reports:

Phone numbers:

Main:

Home:

Mobile:

Add...

Remove

More Information

OK

Cancel

Chapter 7: Managing Active Directory Groups

New Object - Group

Create in:

Group name:

Group name (pre-Windows 2000):

Group scope

☐ Domain local

☒ Global

☐ Universal

Group type

☒ Security

☐ Distribution

OK Cancel

Create Group:

TASKS SECTIONS

* Group

Managed By

Member Of

Members

Password Settings

Group

Group name: *

Group (SamAcco...): *

Group type:

☒ Security

☐ Distribution

Group scope:

☐ Domain local

☒ Global

☐ Universal

☐ Protect from accidental deletion

E-mail:

Create in:

Description: [Change...](#)

Notes:

Managed By

Managed by: [Edit...](#) [Clear](#)

☐ Manager can update membership list

Phone numbers:

Main:

Mobile:

Fax:

Office:

Address:

Street:

City: State/Province: Zip/Postal code:

Country/Region:

Member Of

More Information

OK Cancel

Group Properties ? X

General	Members	Member Of	Managed By
Object	Security	Attribute Editor	

Canonical name of object:

Object class: Group

Created: 1/9/2022 1:46:30 PM

Modified: 1/9/2022 1:46:30 PM

Update Sequence Numbers (USNs):

Current: 28724

Original: 28724

☐ Protect object from accidental deletion

OK Cancel Apply Help

Select Groups X

Select this object type:

Groups or Built-in security principals Object Types...

From this location:

Locations...

Enter the object names to select (examples):

Check Names

Advanced... OK Cancel

Group

TASKS ▾

SECTIONS ▾

Group

Managed By

Member Of

Members

Password Settings

Extensions

Members

Filter

Active Director...

Add...

Remove

Directly Associated Password Settings

Name

Precedence

Assign...

Clear

Extensions

Security

Attribute Editor

More Information

OK

Cancel

Group Properties

?

×

Object

Security


Attribute Editor

General

Members

Member Of

Managed By

 Group

Group name (pre-Windows 2000):

Description:

E-mail:

Group scope

☐ Domain local

☒ Global

☐ Universal

Group type

☒ Security

☐ Distribution

Notes:

OK

Cancel

Apply

Help

Group

TASKS

SECTIONS

Group

Managed By

Member Of

Members

Password Settings

Extensions

Group

Group name: * Group

Group (SamAcco... * Group

Group type:

Security

Distribution

Group scope:

Domain local

Global

Universal

Protect from accidental deletion

E-mail:

Description:

Notes:

Managed By

Managed by:

Edit...

Clear

Manager can update membership list

Phone numbers:

Main:

Mobile:

Fax:

Office:

Address:

Street

City

State/Province

Zip/Postal code

Country/Region:

Member Of

Filter

More Information

OK

Cancel

Chapter 8: Managing Active Directory Computers

New Object - Computer

Create in:

Computer name:

Computer name (pre-Windows 2000):

The following user or group can join this computer to a domain.

User or group:

Default: Domain Admins

Change...

☐ Assign this computer account as a pre-Windows 2000 computer

OK Cancel Help

Create Computer:

TASKS SECTIONS

* Computer

Managed By

Member Of

Policy

Silo

Computer

Computer name: *

Computer (NetBIOS) name: *

Create in: Change...

User or Group: Default: Domain Admins Change ...

The above user or group can join this computer to a domain

☐ Assign this computer account as a Pre-Windows 2000 computer

☐ Protect from accidental deletion

Managed By

Managed by: Edit... Clear Office:

Phone numbers:

Main:

Mobile:

Fax:

Address:

Street

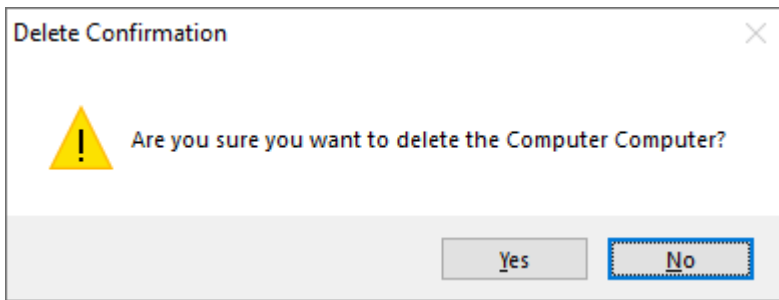
City State/Province Zip/Postal code

Country/Region:

Member Of

More Information

OK Cancel



Computer

TASKS ▼ SECTIONS ▼

Computer

Managed By

Member Of

Policy

Silo

Delegation

Extensions

Computer name: Computer Computer (NetB... COMPUTER)

DNS name:

OS name:

Domain controller... Workstation or server OS version:

Site:

Service pack:

Description:

☐ Protect from accidental deletion

Managed By

Managed by: Edit... Clear Office:

Phone numbers:

Main: Address:

Mobile:

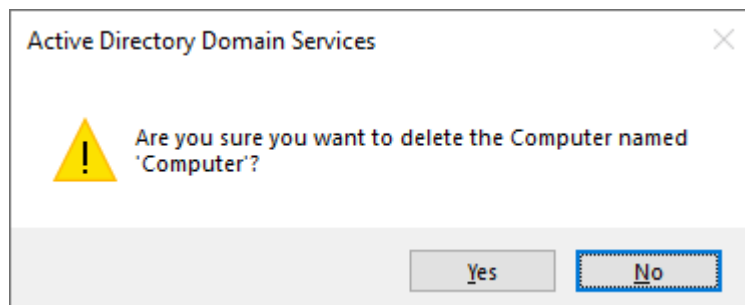
Fax: City State/Province Zip/Postal code

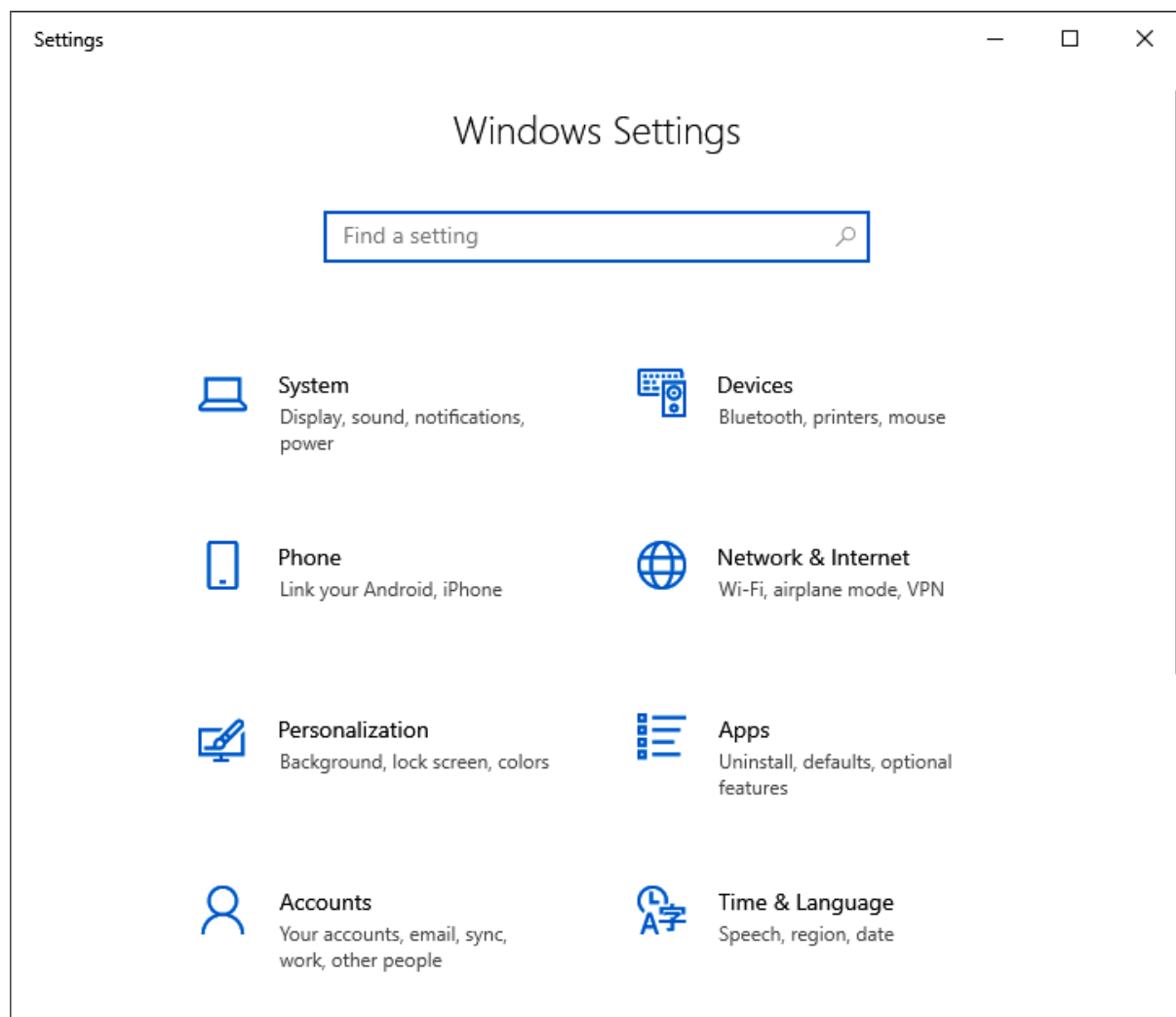
Country/Region:

Member Of

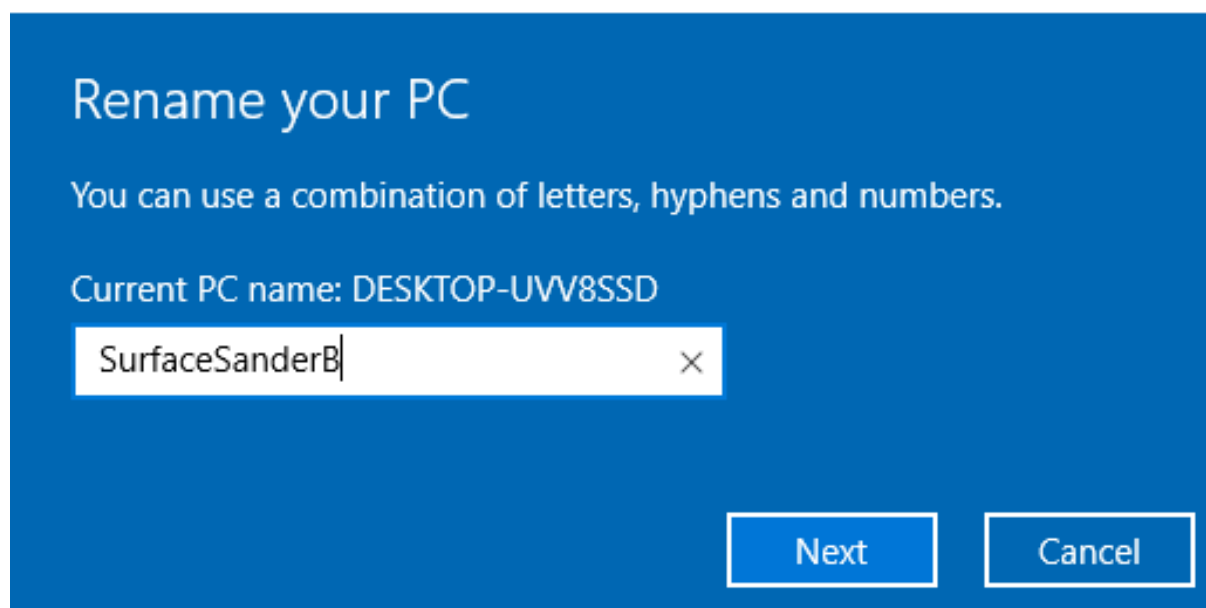
More Information

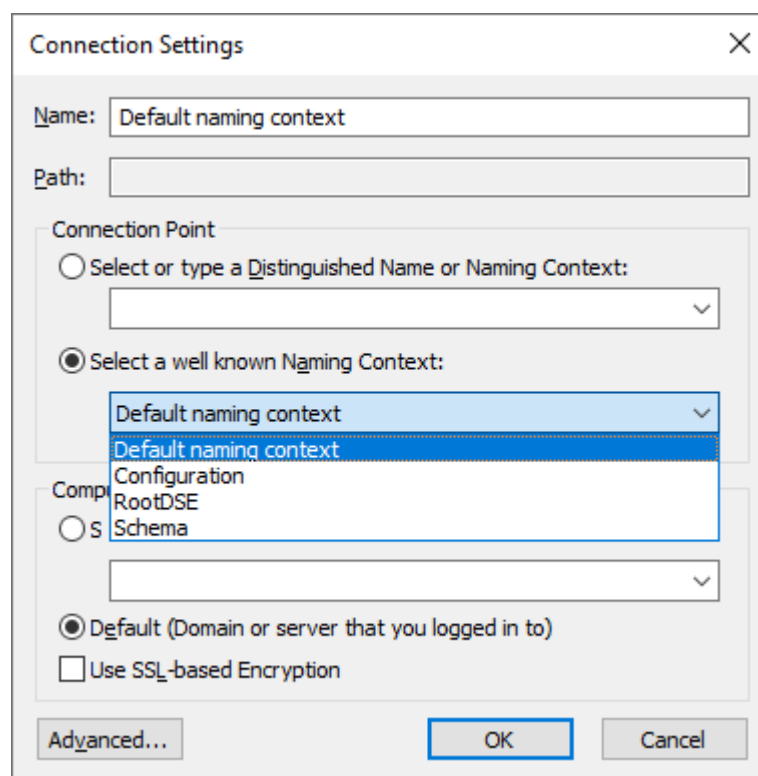
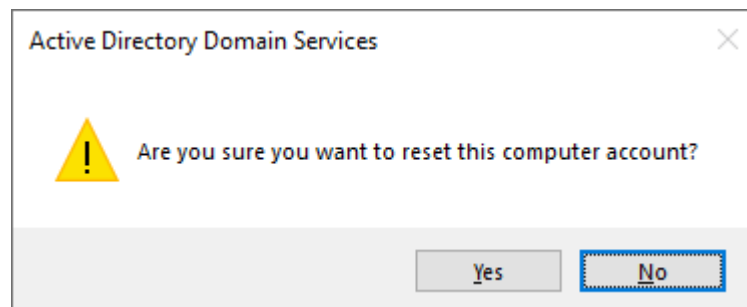
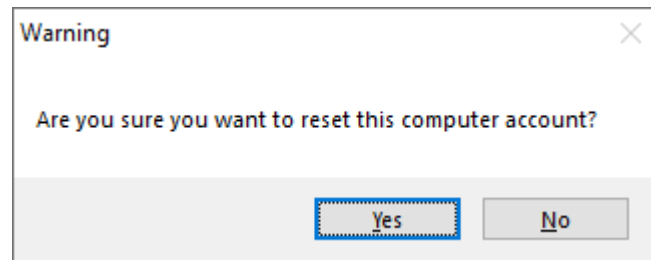
OK Cancel

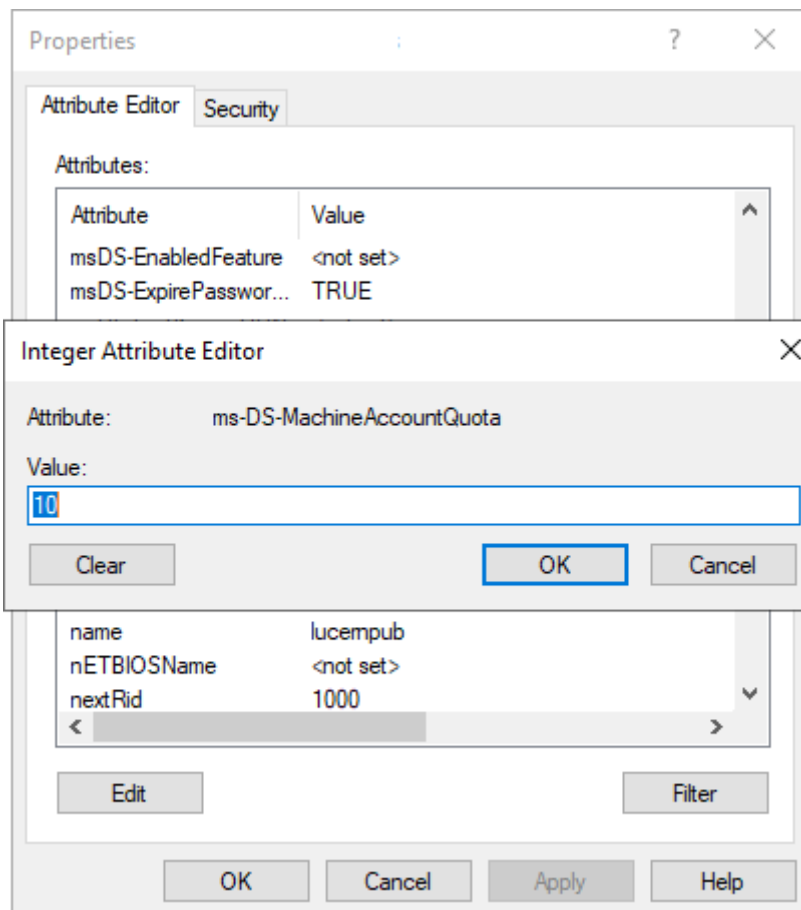




Rename your PC







Chapter 9: Managing DNS

Active Directory Domain Services Configuration Wizard

Domain Controller Options

TARGET SERVER
DC01

Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results

Select functional level of the new forest and root domain

Forest functional level: Windows Server 2016

Domain functional level: Windows Server 2016

Specify domain controller capabilities

☒ Domain Name System (DNS) server

☒ Global Catalog (GC)

☐ Read only domain controller (RODC)

Type the Directory Services Restore Mode (DSRM) password

Password: *

Confirm password: *

[More about domain controller options](#)

< Previous Next > Install Cancel

New Zone Wizard

Zone Type

The DNS server supports various types of zones and storage.

Select the type of zone you want to create:

☒ Primary zone
Creates a copy of a zone that can be updated directly on this server.

☐ Secondary zone
Creates a copy of a zone that exists on another server. This option helps balance the processing load of primary servers and provides fault tolerance.

☐ Stub zone
Creates a copy of a zone containing only Name Server (NS), Start of Authority (SOA), and possibly glue Host (A) records. A server containing a stub zone is not authoritative for that zone.

☒ Store the zone in Active Directory (available only if DNS server is a writeable domain controller)

< Back Next > Cancel

New Zone Wizard

Active Directory Zone Replication Scope

You can select how you want DNS data replicated throughout your network.

Select how you want zone data replicated:

☐ To all DNS servers running on domain controllers in this forest: lucernpub.com

☒ To all DNS servers running on domain controllers in this domain: lucernpub.com

☐ To all domain controllers in this domain (for Windows 2000 compatibility): lucernpub.com

☐ To all domain controllers specified in the scope of this directory partition:

< Back

Next >

Cancel

New Zone Wizard

Dynamic Update

You can specify that this DNS zone accepts secure, nonsecure, or no dynamic updates.

Dynamic updates enable DNS client computers to register and dynamically update their resource records with a DNS server whenever changes occur.

Select the type of dynamic updates you want to allow:

☒ Allow only secure dynamic updates (recommended for Active Directory)

This option is available only for Active Directory-integrated zones.

☐ Allow both nonsecure and secure dynamic updates

Dynamic updates of resource records are accepted from any client.

!

 This option is a significant security vulnerability because updates can be accepted from untrusted sources.

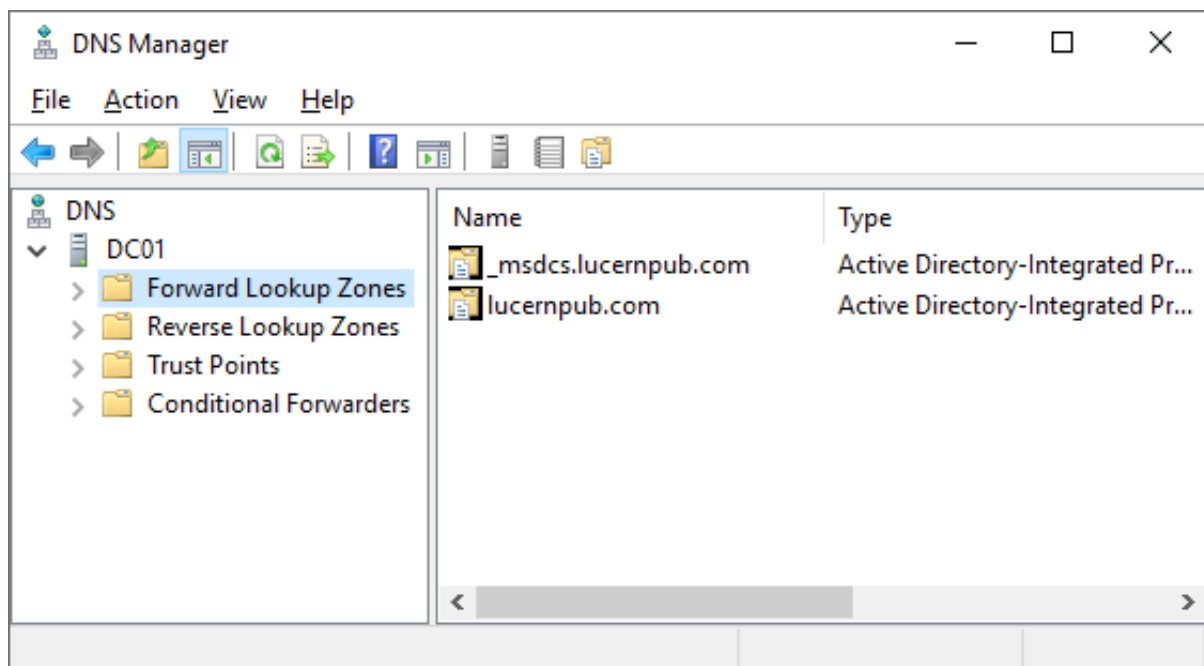
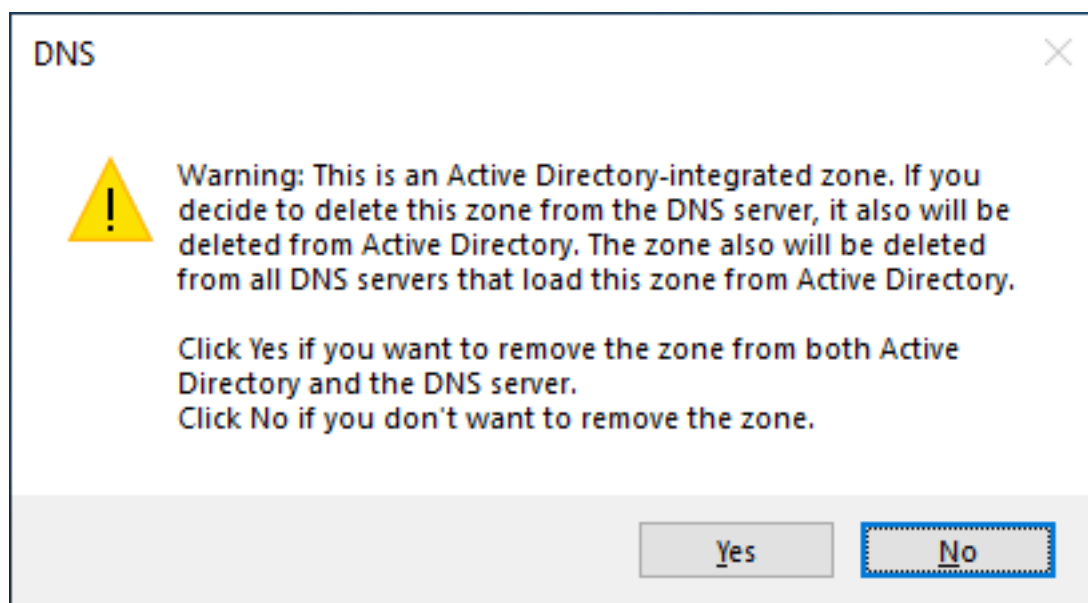
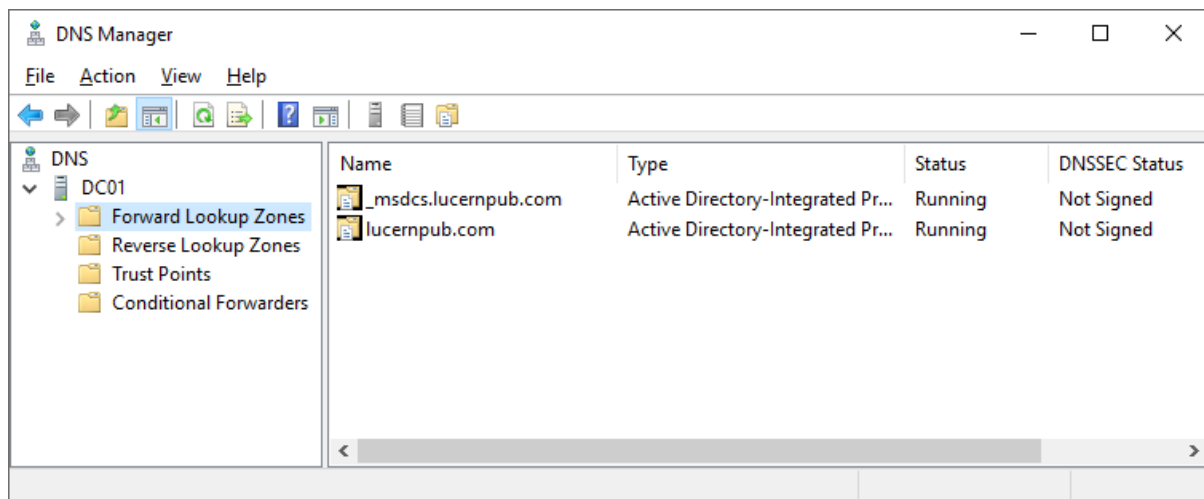
☐ Do not allow dynamic updates

Dynamic updates of resource records are not accepted by this zone. You must update these records manually.

< Back

Next >

Cancel



```
netlogon.dns - Notepad
File Edit Format View Help
lucernpub.com. 600 IN A 10.0.0.4
_ldap._tcp.lucernpub.com. 600 IN SRV 0 100 389 dc01.lucernpub.com.
_ldap._tcp.Default-First-Site-Name._sites.lucernpub.com. 600 IN SRV 0 100 389 dc01.lucernpub.com.
_ldap._tcp.pdc._msdcs.lucernpub.com. 600 IN SRV 0 100 389 dc01.lucernpub.com.
_ldap._tcp.1a78ff72-a762-46d5-b919-5fdfccb23f8e.domains._msdcs.lucernpub.com. 600 IN SRV 0 100 389 dc01.lucernpub.com.
a699713e-f94f-4496-ae01-f1f9ac9b978b._msdcs.lucernpub.com. 600 IN CNAME dc01.lucernpub.com.
_ldap._tcp.dc._msdcs.lucernpub.com. 600 IN SRV 0 100 389 dc01.lucernpub.com.
_ldap._tcp.Default-First-Site-Name._sites.dc._msdcs.lucernpub.com. 600 IN SRV 0 100 389 dc01.lucernpub.com.
_ldap._tcp.gc._msdcs.lucernpub.com. 600 IN SRV 0 100 3268 dc01.lucernpub.com.
_ldap._tcp.Default-First-Site-Name._sites.gc._msdcs.lucernpub.com. 600 IN SRV 0 100 3268 dc01.lucernpub.com.
gc._msdcs.lucernpub.com. 600 IN A 10.0.0.4
_kerberos._tcp.dc._msdcs.lucernpub.com. 600 IN SRV 0 100 88 dc01.lucernpub.com.
_kerberos._tcp.Default-First-Site-Name._sites.dc._msdcs.lucernpub.com. 600 IN SRV 0 100 88 dc01.lucernpub.com.
_kerberos._tcp.lucernpub.com. 600 IN SRV 0 100 88 dc01.lucernpub.com.
_kerberos._tcp.Default-First-Site-Name._sites.lucernpub.com. 600 IN SRV 0 100 88 dc01.lucernpub.com.
_gc._tcp.lucernpub.com. 600 IN SRV 0 100 3268 dc01.lucernpub.com.
_gc._tcp.Default-First-Site-Name._sites.lucernpub.com. 600 IN SRV 0 100 3268 dc01.lucernpub.com.
_kerberos._udp.lucernpub.com. 600 IN SRV 0 100 88 dc01.lucernpub.com.
_kpasswd._tcp.lucernpub.com. 600 IN SRV 0 100 464 dc01.lucernpub.com.
_kpasswd._udp.lucernpub.com. 600 IN SRV 0 100 464 dc01.lucernpub.com.
DomainDnsZones.lucernpub.com. 600 IN A 10.0.0.4
_ldap._tcp.Default-First-Site-Name._sites.DomainDnsZones.lucernpub.com. 600 IN SRV 0 100 389 dc01.lucernpub.com.
ForestDnsZones.lucernpub.com. 600 IN A 10.0.0.4
_ldap._tcp.ForestDnsZones.lucernpub.com. 600 IN SRV 0 100 389 dc01.lucernpub.com.
_ldap._tcp.Default-First-Site-Name._sites.ForestDnsZones.lucernpub.com. 600 IN SRV 0 100 389 dc01.lucernpub.com.
_ldap._tcp.DomainDnsZones.lucernpub.com. 600 IN SRV 0 100 389 dc01.lucernpub.com.
```

New Conditional Forwarder

DNS Domain:

IP addresses of the master servers:

IP Address	Server FQDN	Validated
<Click here to add a...>		

Delete

Up

Down

☐ Store this conditional forwarder in Active Directory, and replicate it as follows:

All DNS servers in this forest

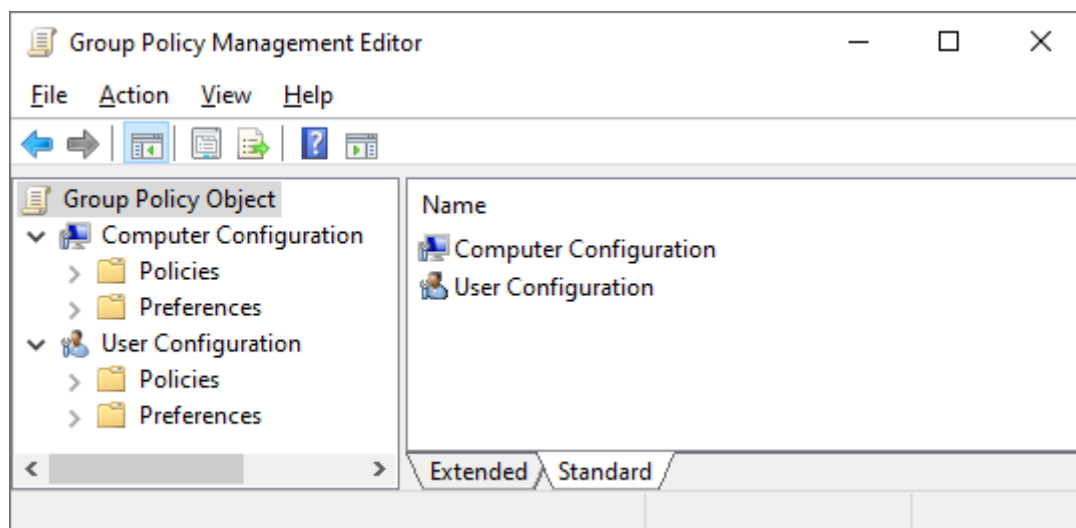
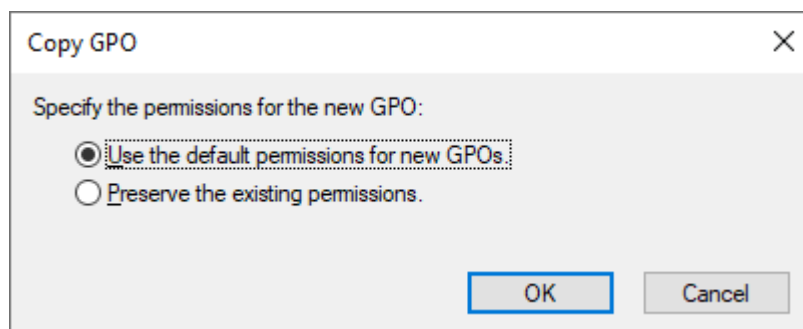
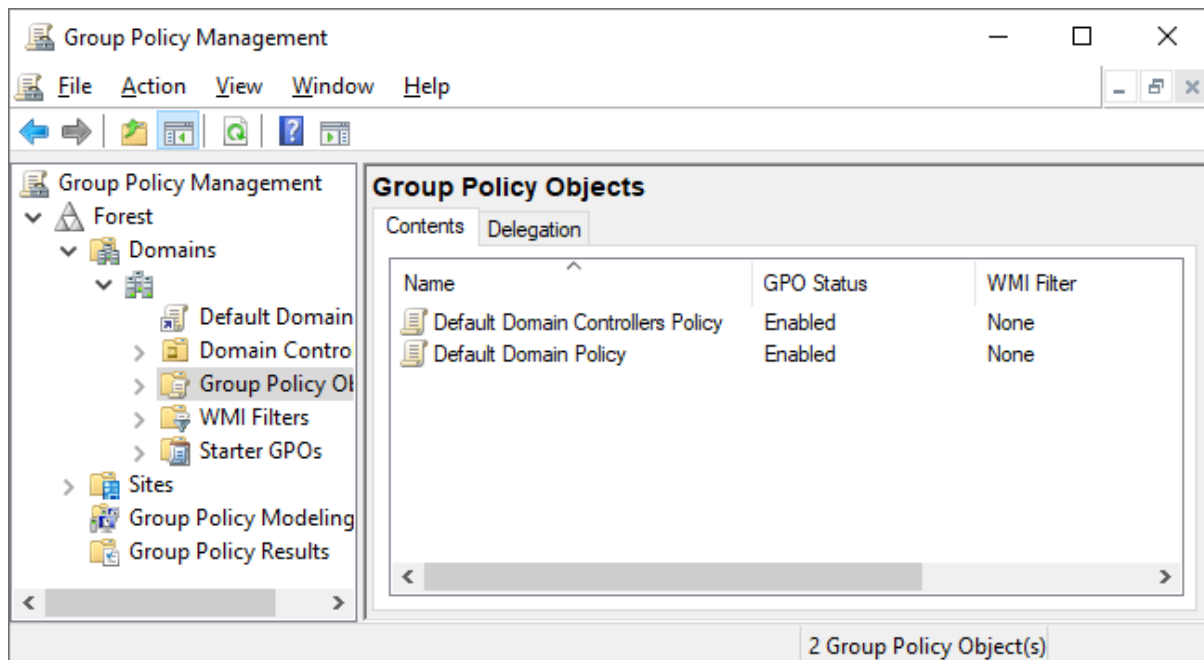
Number of seconds before forward queries time out: 5

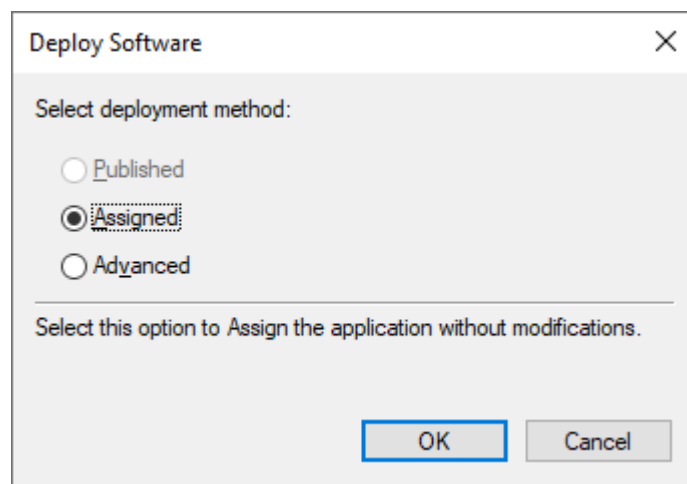
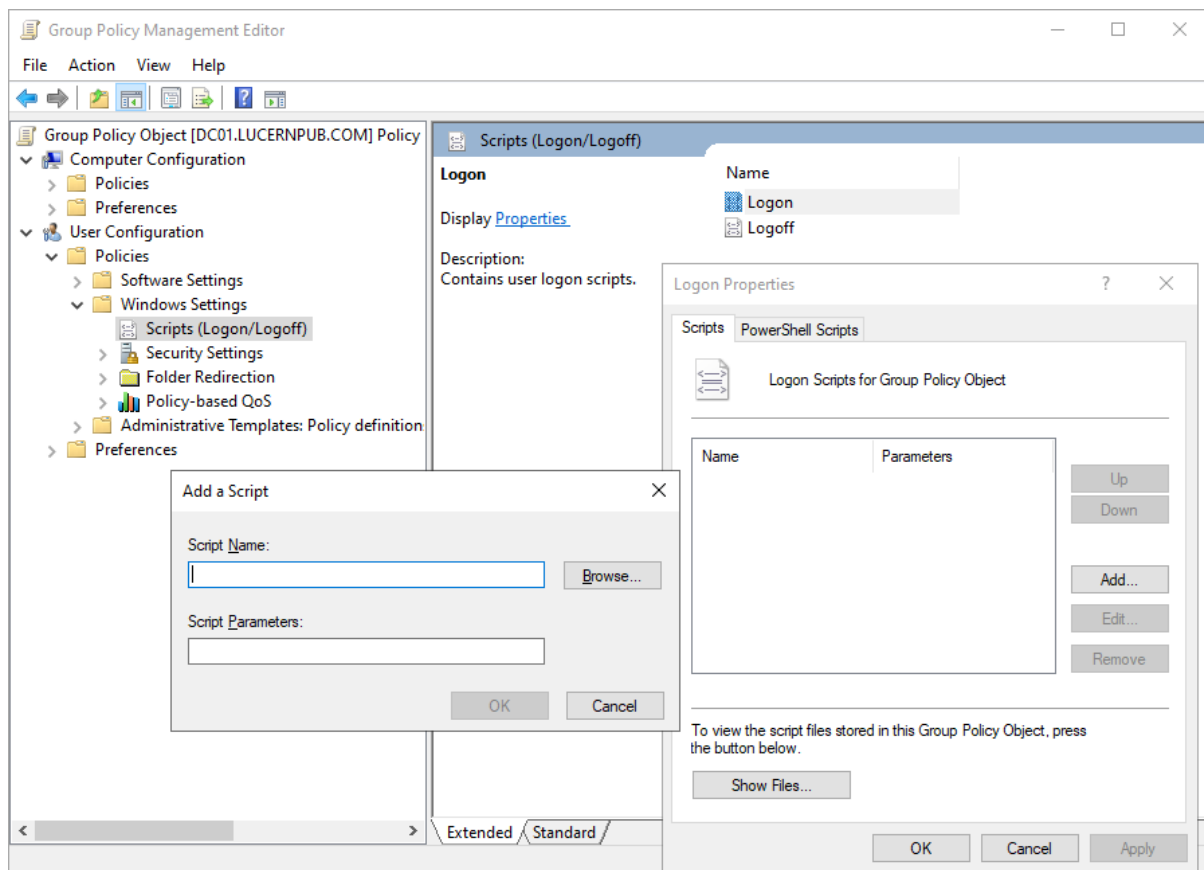
The server FQDN will not be available if the appropriate reverse lookup zones and entries are not configured.

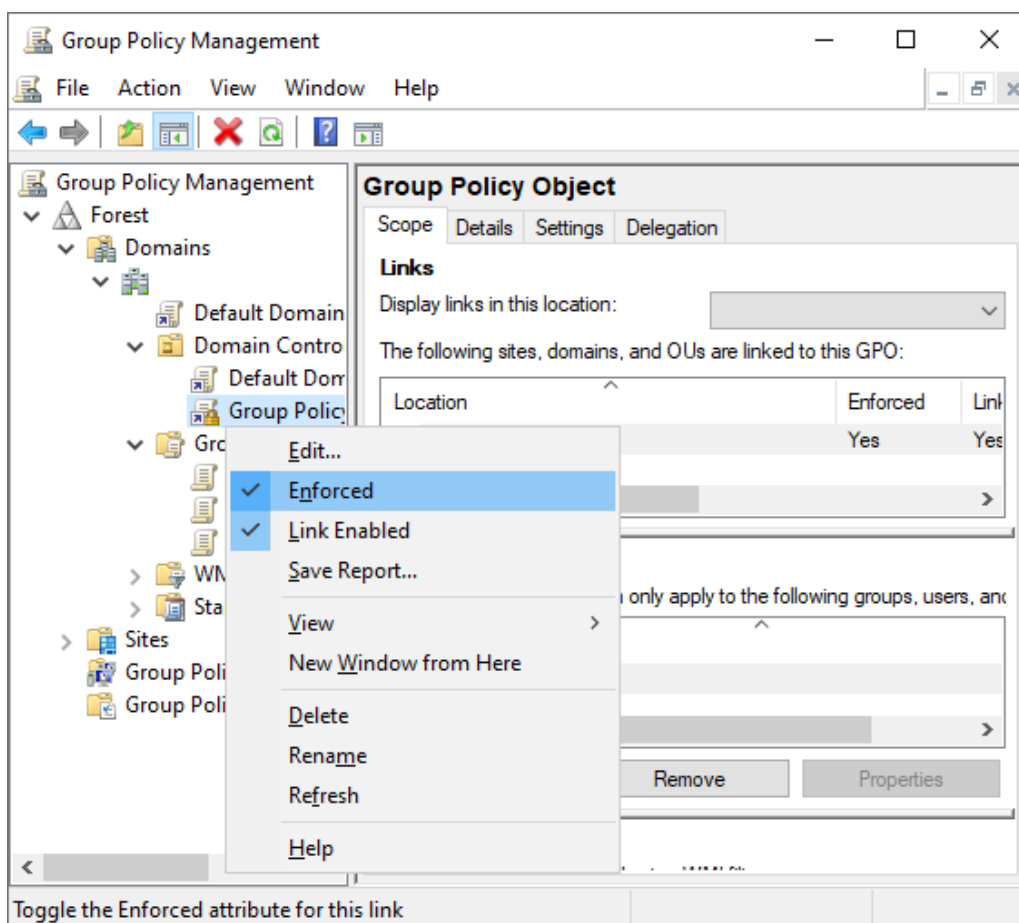
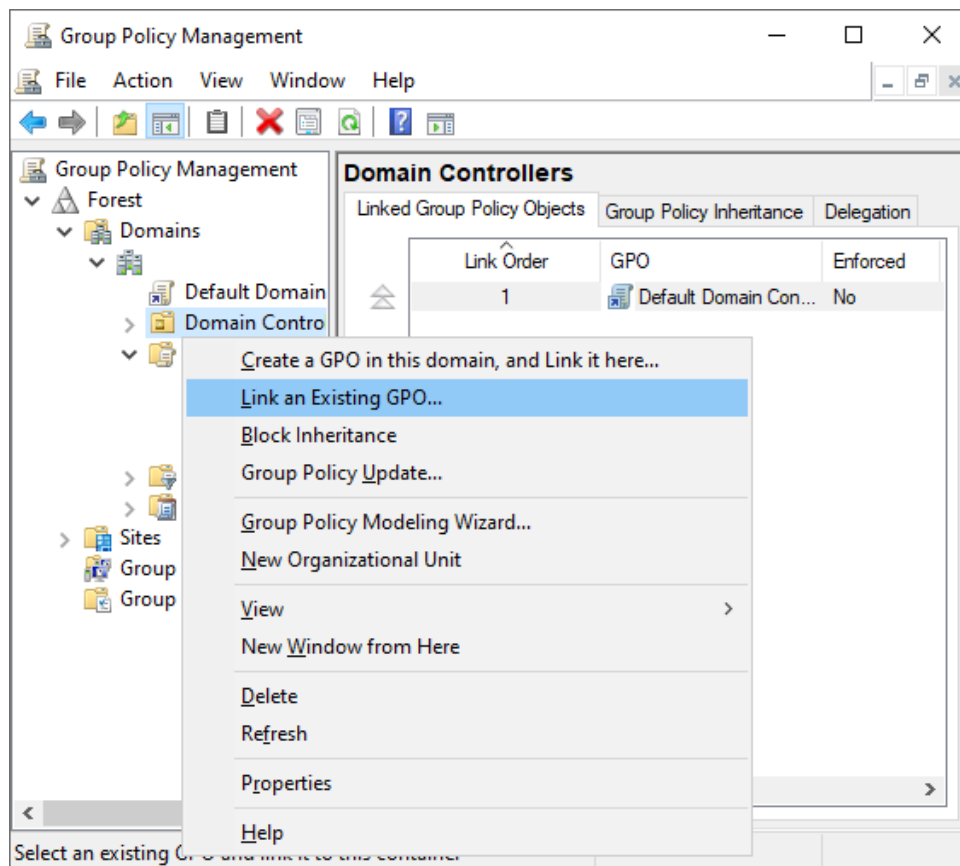
OK

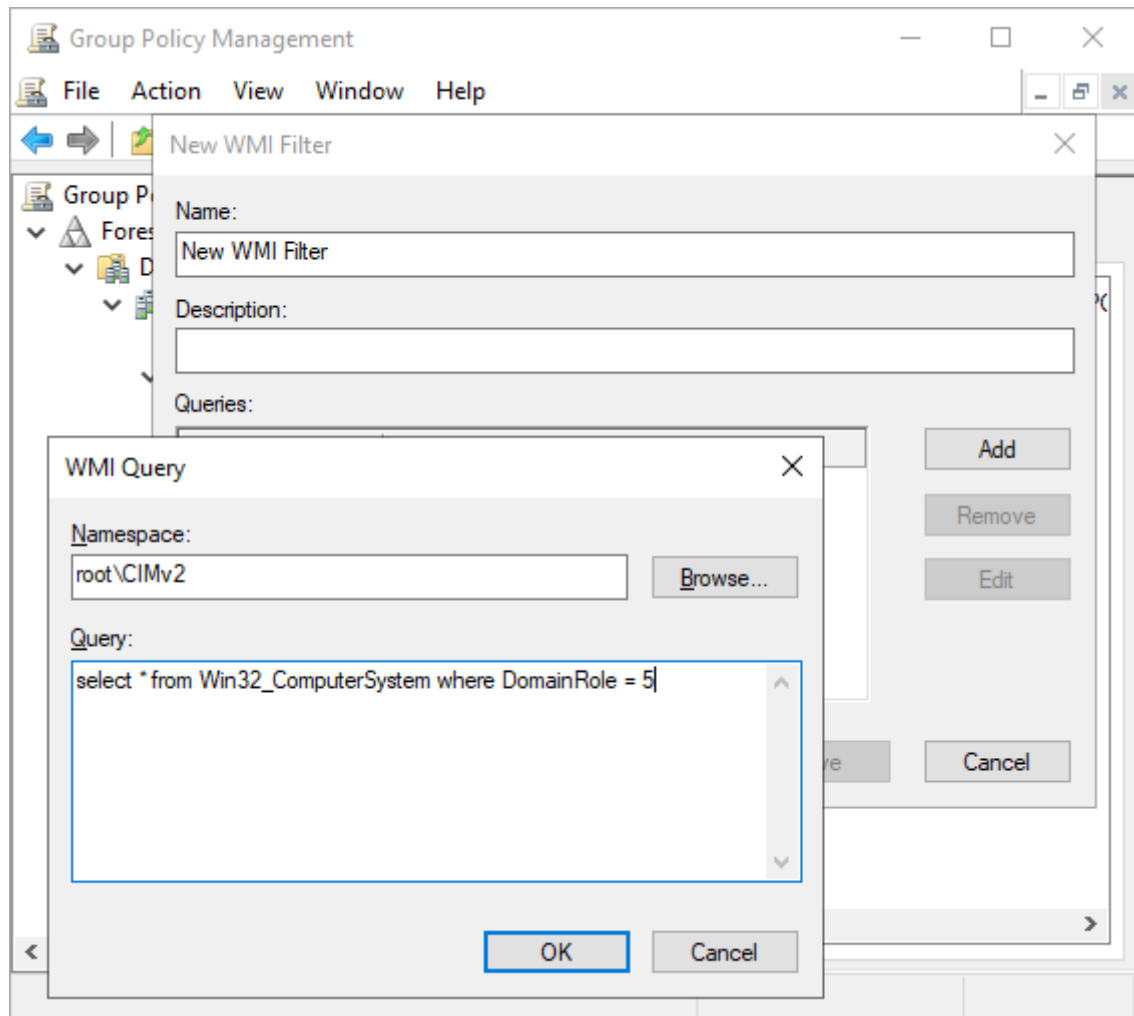
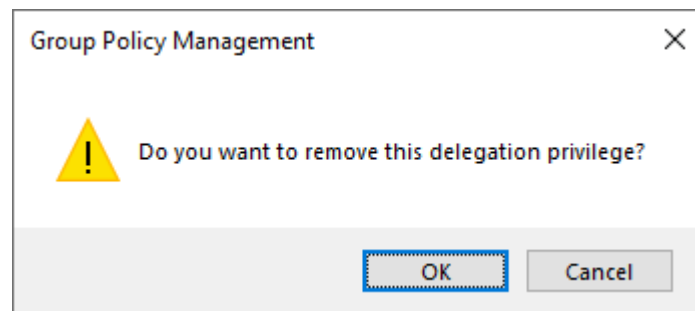
Cancel

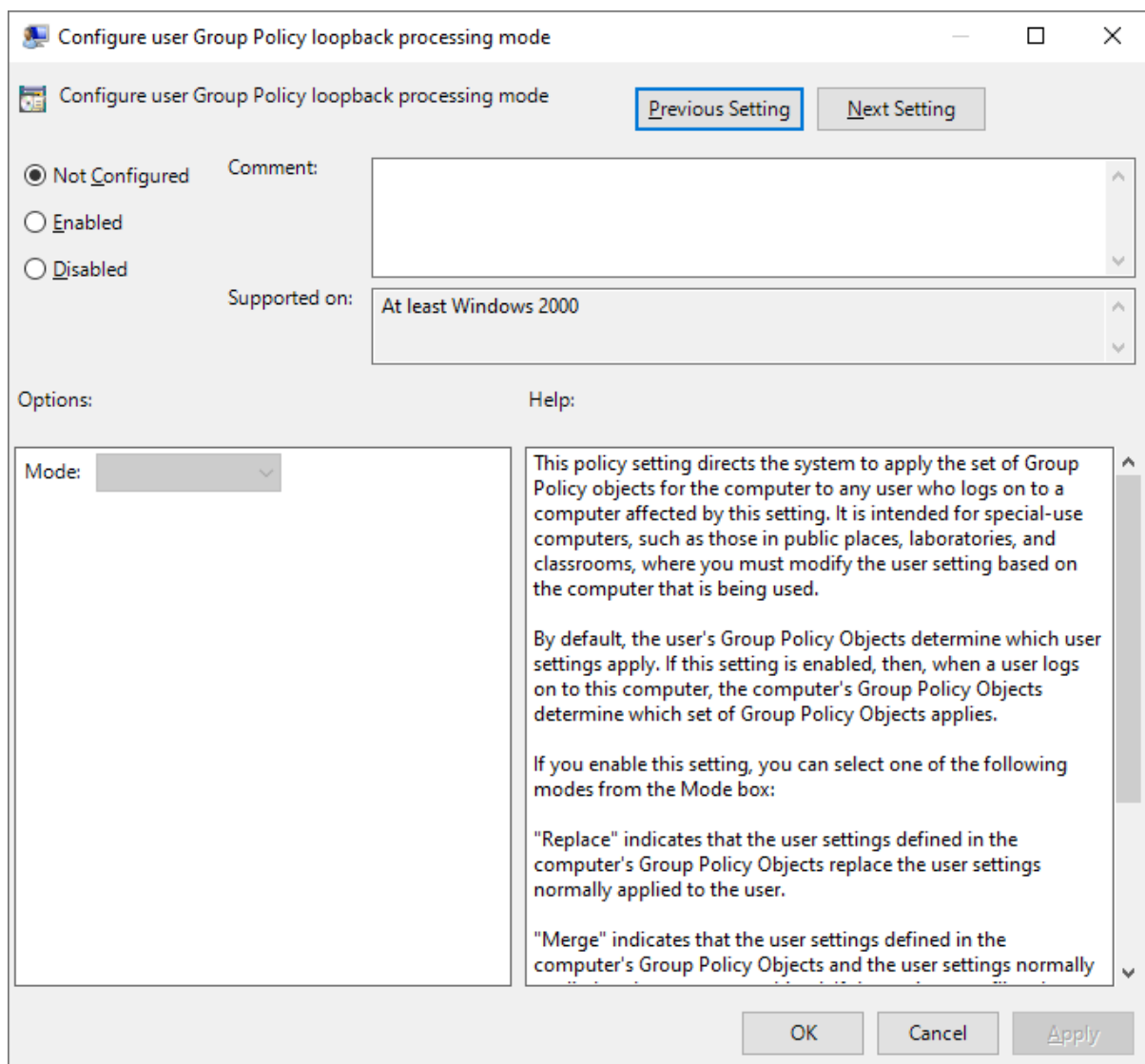
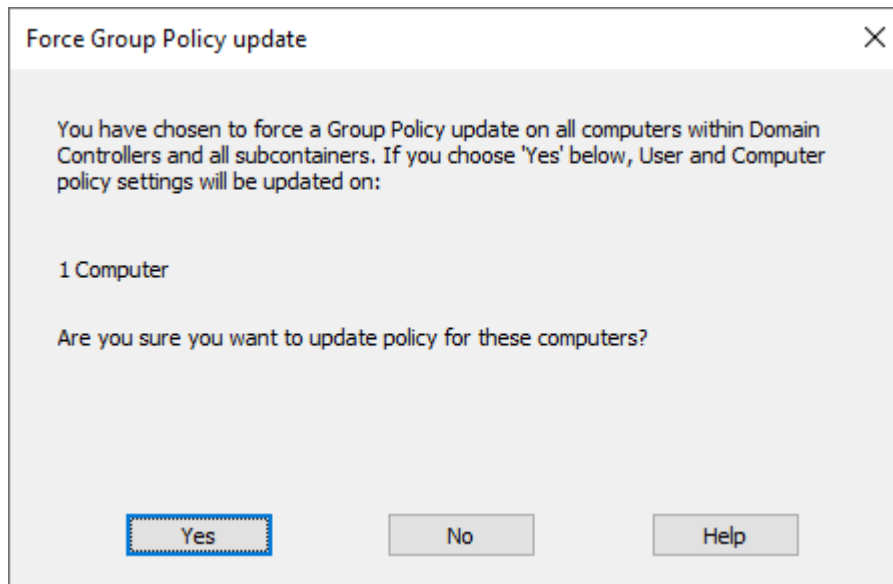
Chapter 10: Getting the Most Out of Group Policy



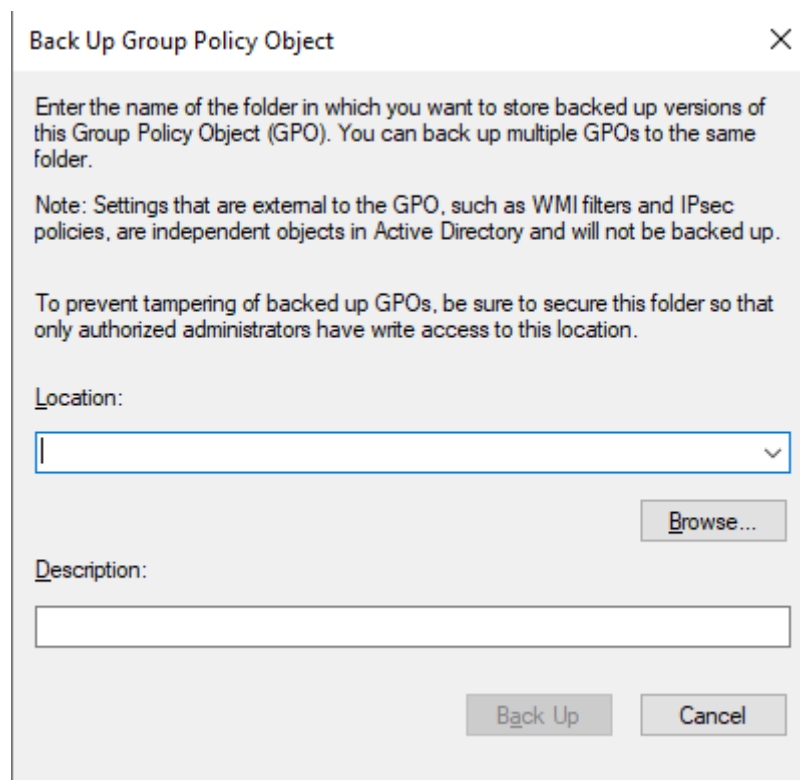
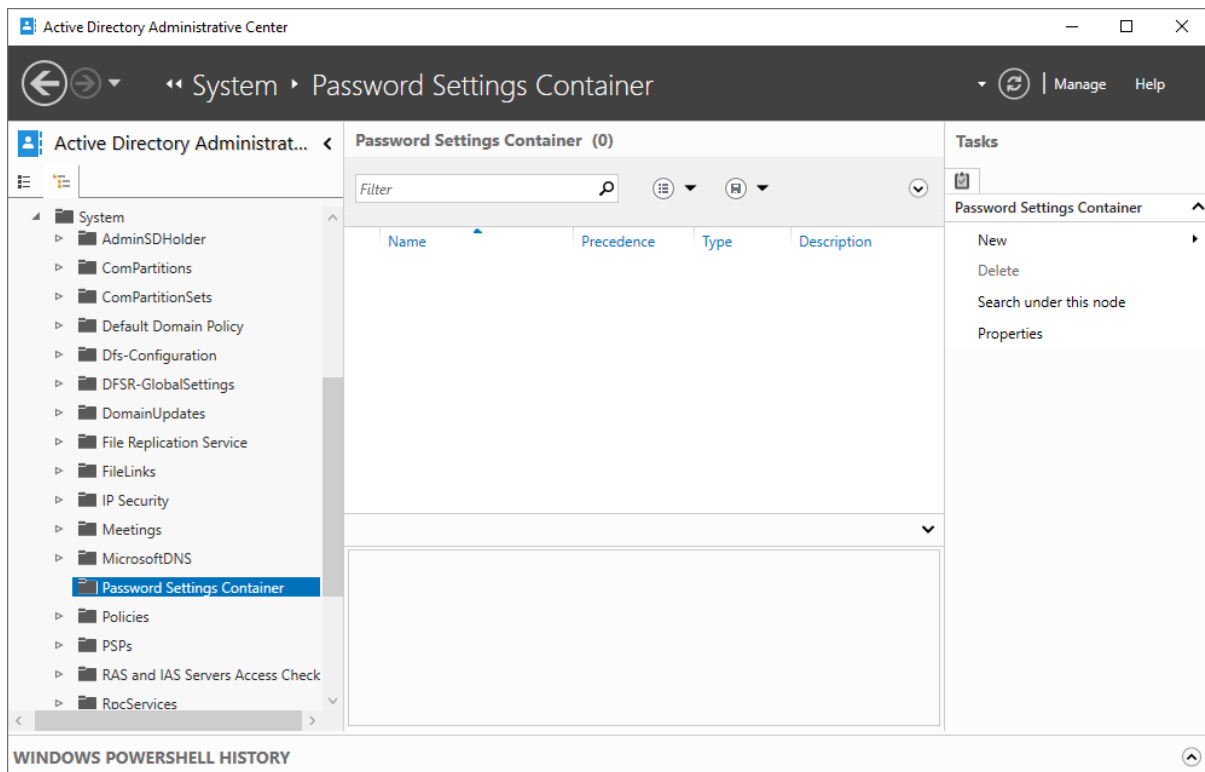


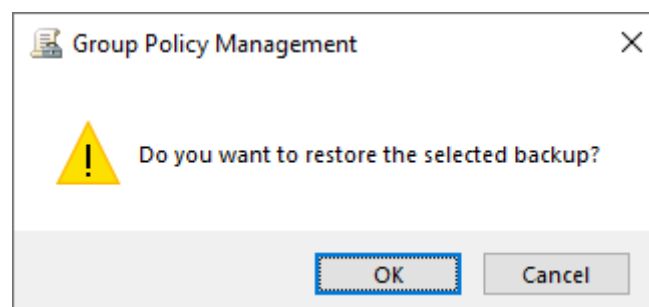


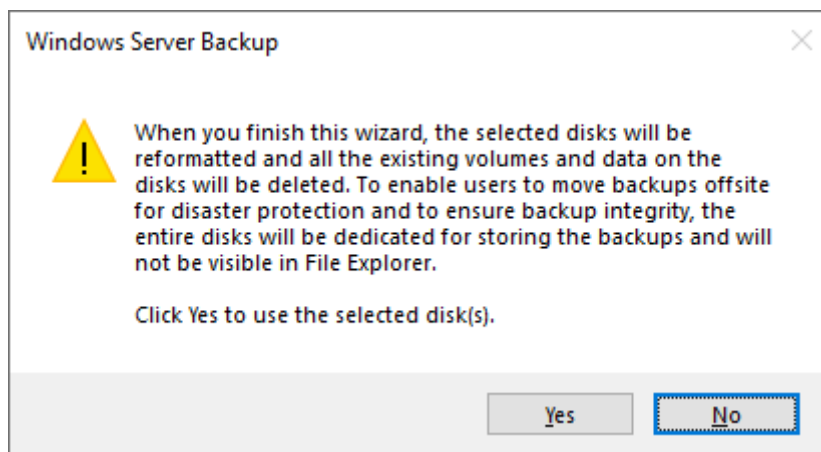
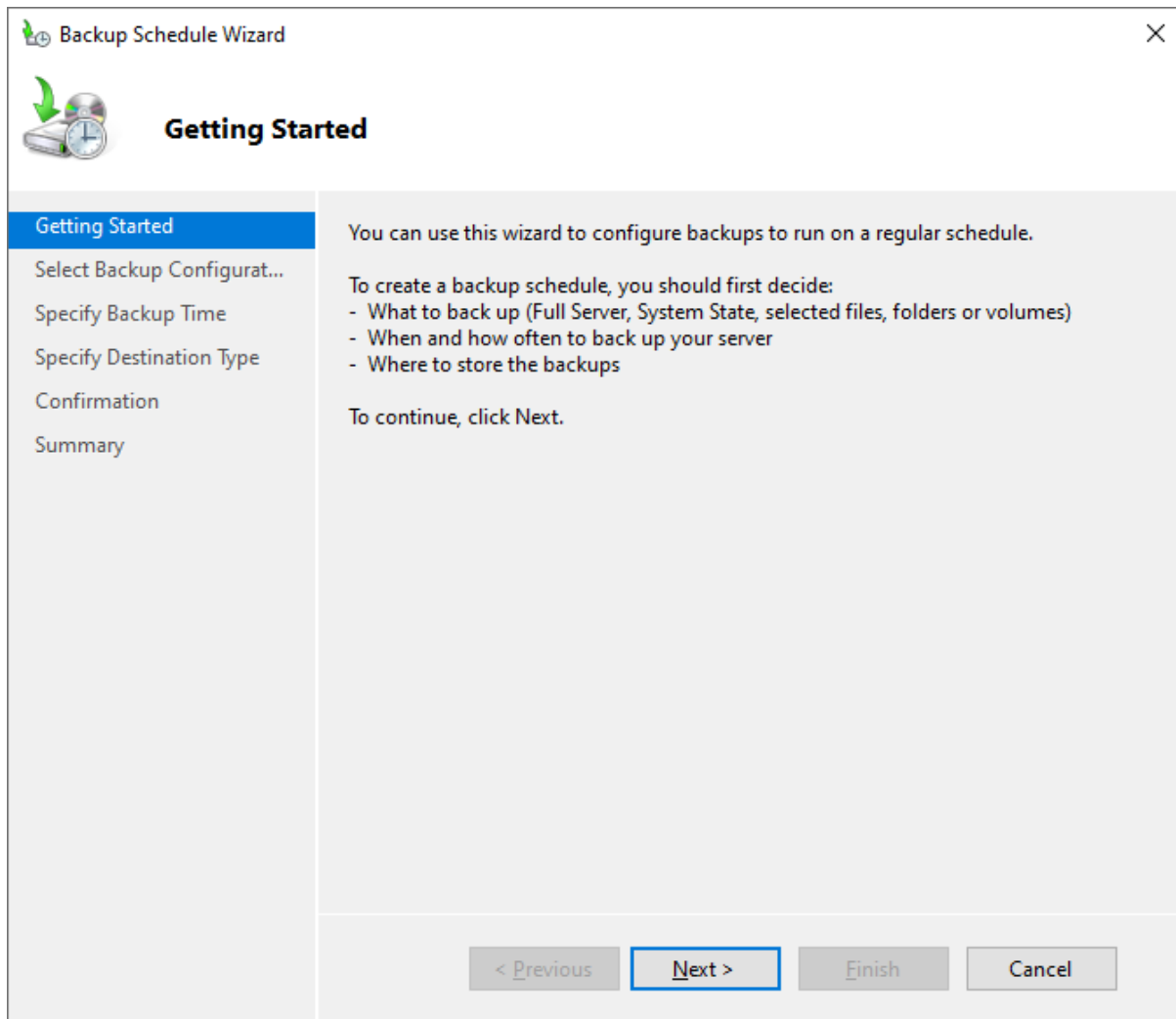





Chapter 11: Securing Active Directory







Recovery Wizard



Getting Started

Getting Started
Select Backup Date
Select Recovery Type
Select Items to Recover
Specify Recovery Options
Confirmation
Recovery Progress

You can use this wizard to recover files, applications, volumes, or the system state from a backup that was created earlier.

Where is the backup stored that you want to use for the recovery?

☒ This server

☐ A backup stored on another location

To continue, click Next.


< Previous

Next >

Recover

Cancel

Recovery Wizard



Select Location for System State Recovery

Getting Started
Select Backup Date
Select Recovery Type
Select Location for System State Recovery
Confirmation
Recovery Progress

Where do you want to recover the system state of this Active Directory backup to?

☒ Original location

This option restores the system state. You must restart your computer at the end of the recovery operation.

☐ Perform an authoritative restore of Active Directory files.

This recovery option will reset all replicated content on this Domain Controller including SYSVOL. Other replicated folders on this server will also be affected by this recovery.

☐ Alternate location

This option copies the system state as a set of files to the location specified.

Browse

☐ Restore as Install From Media (IFM) files

Select this checkbox if you are using the IFM feature to copy the system state files to install an Active Directory database.

< Previous

Next >

Recover

Cancel

Organizational Unit Properties ? X

General Managed By Object Security COM+ Attribute Editor

Canonical name of object:
/Organizational Unit

Object class: Organizational Unit

Created: 2/9/2022 8:24:27 AM

Modified: 2/9/2022 8:24:27 AM

Update Sequence Numbers (USNs):

Current: 57388

Original: 57387

☒ Protect object from accidental deletion


OK Cancel Apply Help

LAPS UI X

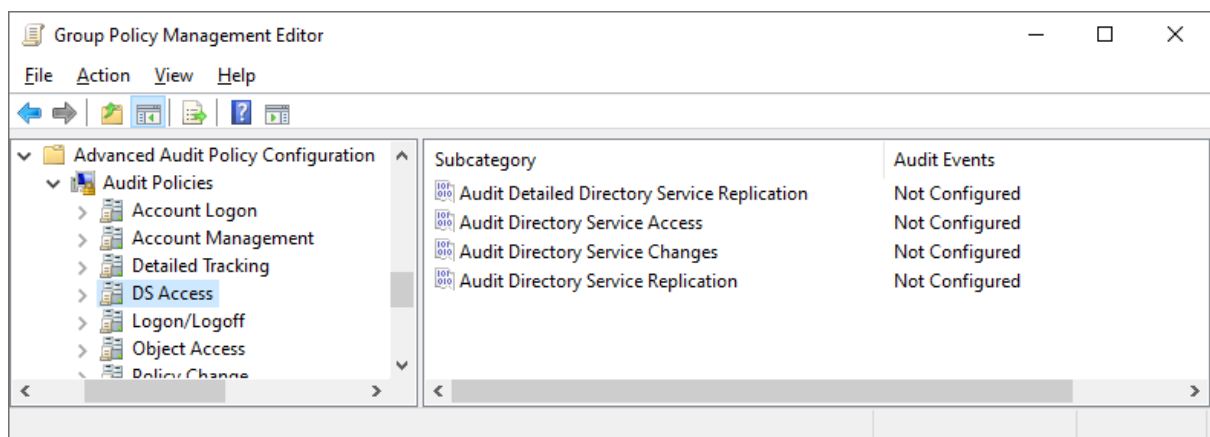
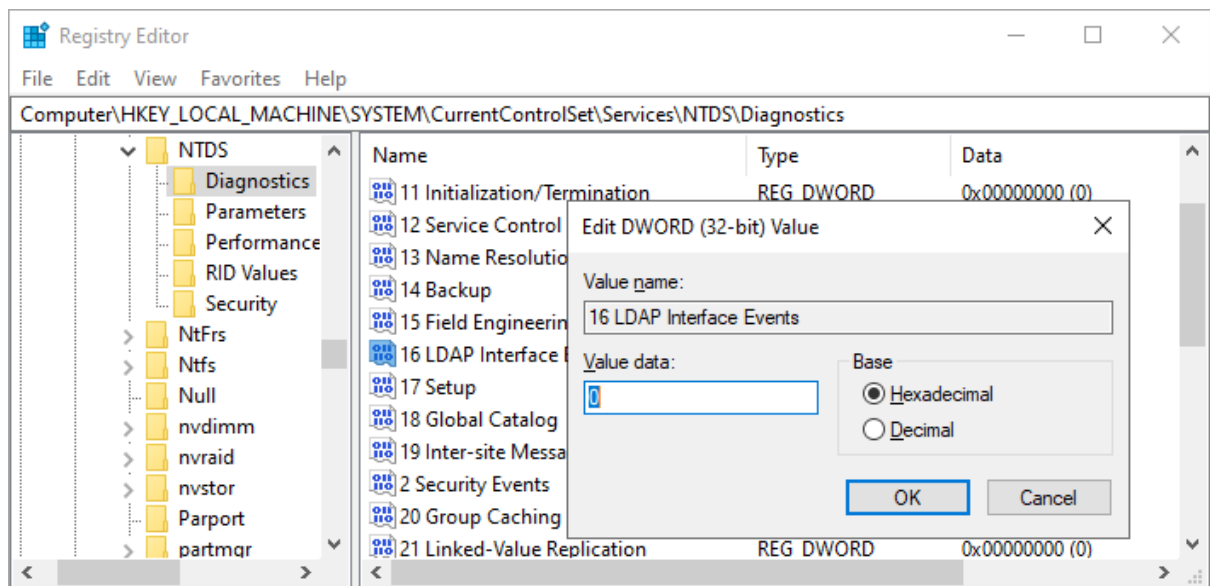
Computer name:
 Search

Password:

Password expires:

New expiration time (leave as is for immediate expiration):
Friday , 4 February 2022 08:53:51  Set

Exit



Protected Users Properties

Select Users, Contacts, Computers, Service Accounts, or Groups

Select this object type:
 Users, Service Accounts, Groups, or Other objects Object Types...

From this location:
Locations...

Enter the object names to select (examples):
 Domain Admins Check Names

Advanced... OK Cancel

Add... Remove

OK Cancel Apply Help

KDC support for claims, compound authentication and Kerberos armoring

KDC support for claims, compound authentication and Kerberos armoring Previous Setting Next Setting

☐ Not Configured Comment:
☒ Enabled
☐ Disabled

Supported on: At least Windows Server 2012, Windows 8 or Windows RT

Options: Help:

Claims, compound authentication for Dynamic Access Control and Kerberos armoring options:
 Supported

This policy setting allows you to configure a domain controller to support claims and compound authentication for Dynamic Access Control and Kerberos armoring using Kerberos authentication.

If you enable this policy setting, client computers that support claims and compound authentication for Dynamic Access Control and are Kerberos armor-aware will use this feature for Kerberos authentication messages. This policy should be applied to all domain controllers to ensure consistent application of this policy in the domain.

If you disable or do not configure this policy setting, the domain controller does not support claims, compound authentication or armoring.

If you configure the "Not supported" option, the domain controller does not support claims, compound authentication or armoring which is the default behavior for domain controllers running Windows Server 2008 R2 or earlier operating systems.

OK Cancel Apply

Kerberos client support for claims, compound authentication and Kerberos armoring

Previous Setting Next Setting

☐ Not Configured
 ☒ Enabled
 ☐ Disabled

Comment:

Supported on: At least Windows Server 2012, Windows 8 or Windows RT

Options:

Help:

This policy setting controls whether a device will request claims and compound authentication for Dynamic Access Control and Kerberos armoring using Kerberos authentication with domains that support these features.

If you enable this policy setting, the client computers will request claims, provide information required to create compounded authentication and armor Kerberos messages in domains which support claims and compound authentication for Dynamic Access Control and Kerberos armoring.

If you disable or do not configure this policy setting, the client devices will not request claims, provide information required to create compounded authentication and armor Kerberos messages. Services hosted on the device will not be able to retrieve claims for clients using Kerberos protocol transition.

OK Cancel Apply

Create Authentication Policy:

TASKS SECTIONS

* General

Accounts

Silos

User Sign On

Service Tickets for User Accounts

Service Sign On

Service Tickets for Service Accounts

Computer

General

An authentication policy defines the Kerberos Ticket Granting Ticket properties and authentication access control conditions for an account type.

Display name: *

Description:

☐ Only audit policy restrictions
☒ Enforce policy restrictions
 Note: Audit policy applied through a

☒ Protect from accidental deletion

More Information

OK Cancel

Create Authentication Policy Silo:

TASKS

SECTIONS

*

General

Accounts

*

Policy

General

An authentication policy silo controls which accounts are to be protected by the silo and defines the authentication policies to be applied to members of the silo.

Display name:

*

Description:

☒ Protect from accidental deletion

☒ Only audit silo policies

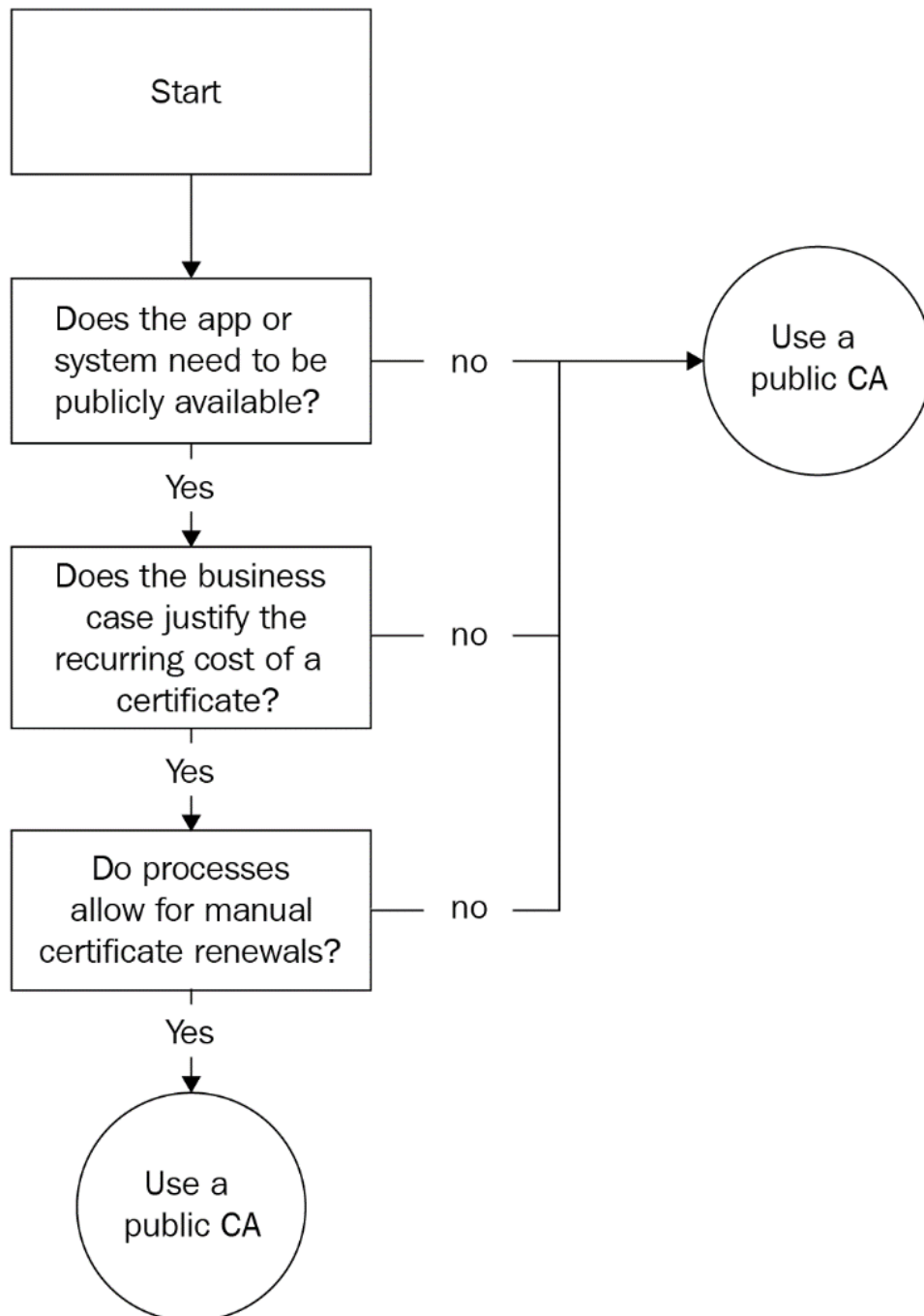
☐ Enforce silo policies

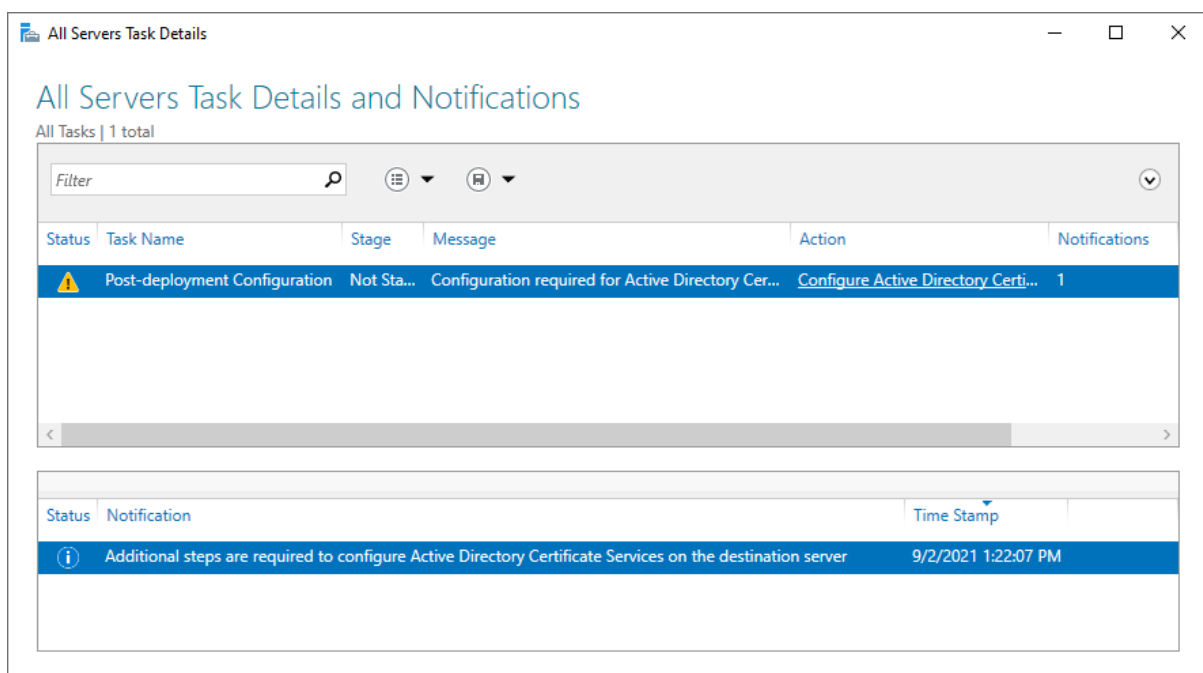
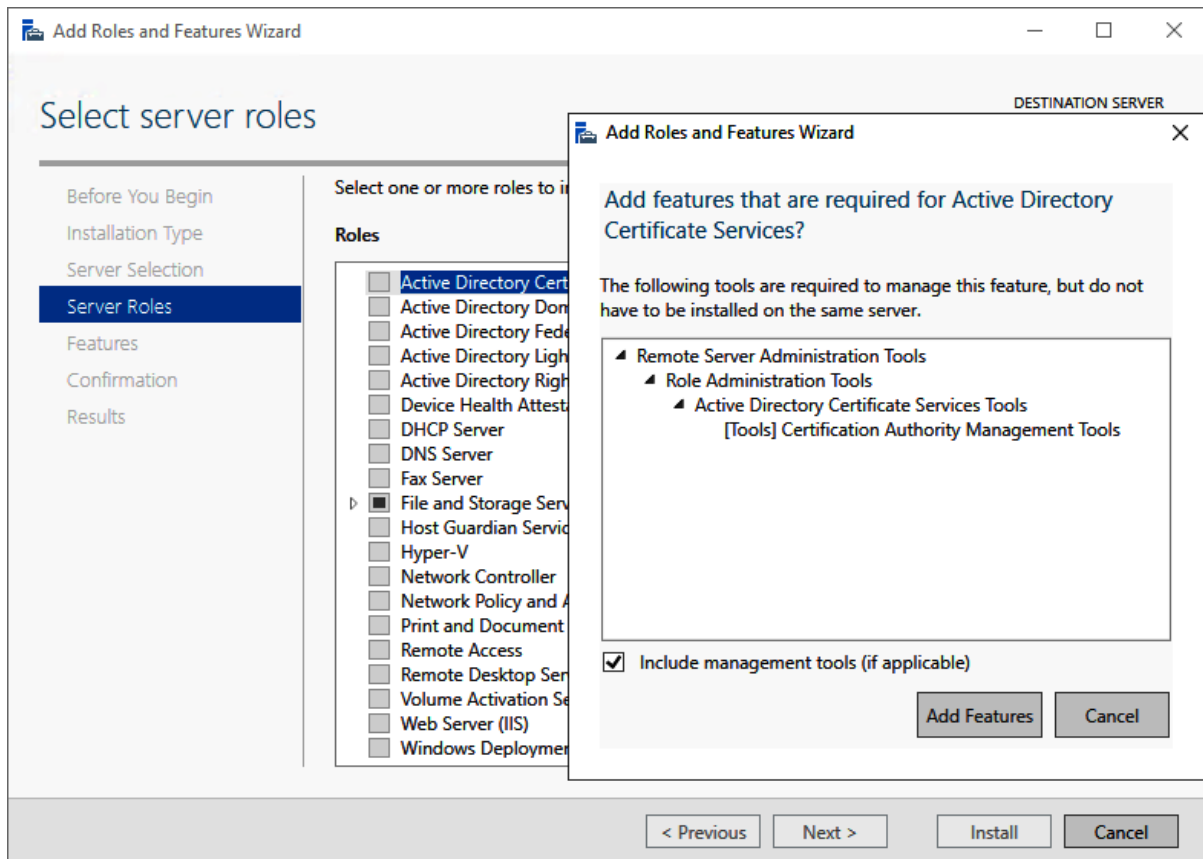
More Information

OK

Cancel

Chapter 12: Managing Certificates





AD CS Configuration

DESTINATION SERVER
CA01

CA Type

Credentials

Role Services

Setup Type

CA Type

Private Key

Cryptography

CA Name

Validity Period

Certificate Database

Confirmation

Progress

Results

Specify the type of the CA

When you install Active Directory Certificate Services (AD CS), you are creating or extending a public key infrastructure (PKI) hierarchy. A root CA is at the top of the PKI hierarchy and issues its own self-signed certificate. A subordinate CA receives a certificate from the CA above it in the PKI hierarchy.

☒ **Root CA**
Root CAs are the first and may be the only CAs configured in a PKI hierarchy.

☐ **Subordinate CA**
Subordinate CAs require an established PKI hierarchy and are authorized to issue certificates by the CA above them in the hierarchy.

[More about CA Type](#)

< Previous

Next >

Configure

Cancel

Add Roles and Features Wizard

DESTINATION SERVER
CA01

Select server roles

Before You Begin

Installation Type

Server Selection

Server Roles

Features

Web Server Role (IIS)

Role Services

Confirmation

Results

Select one or more roles to install on the selected server.

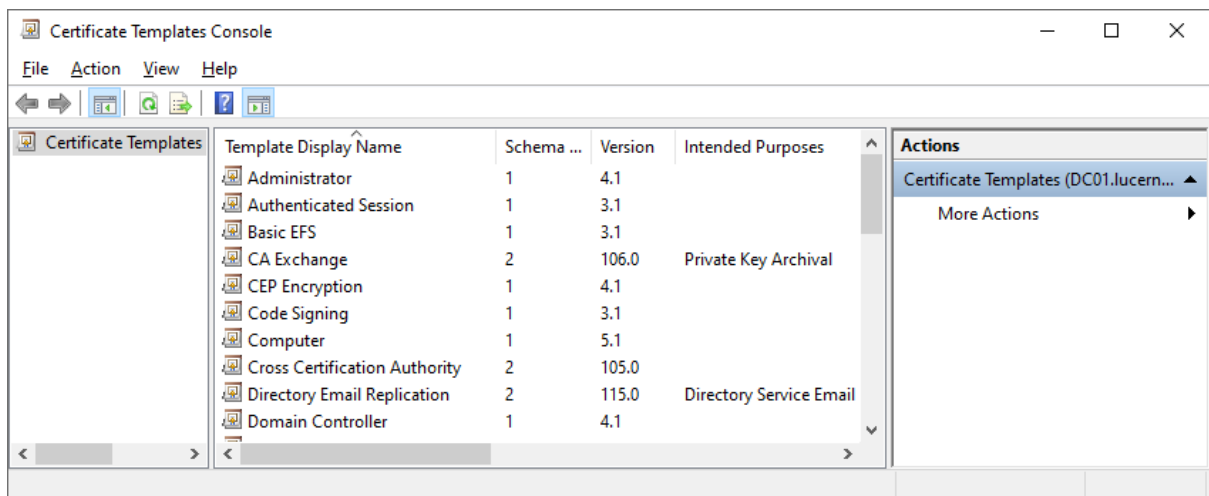
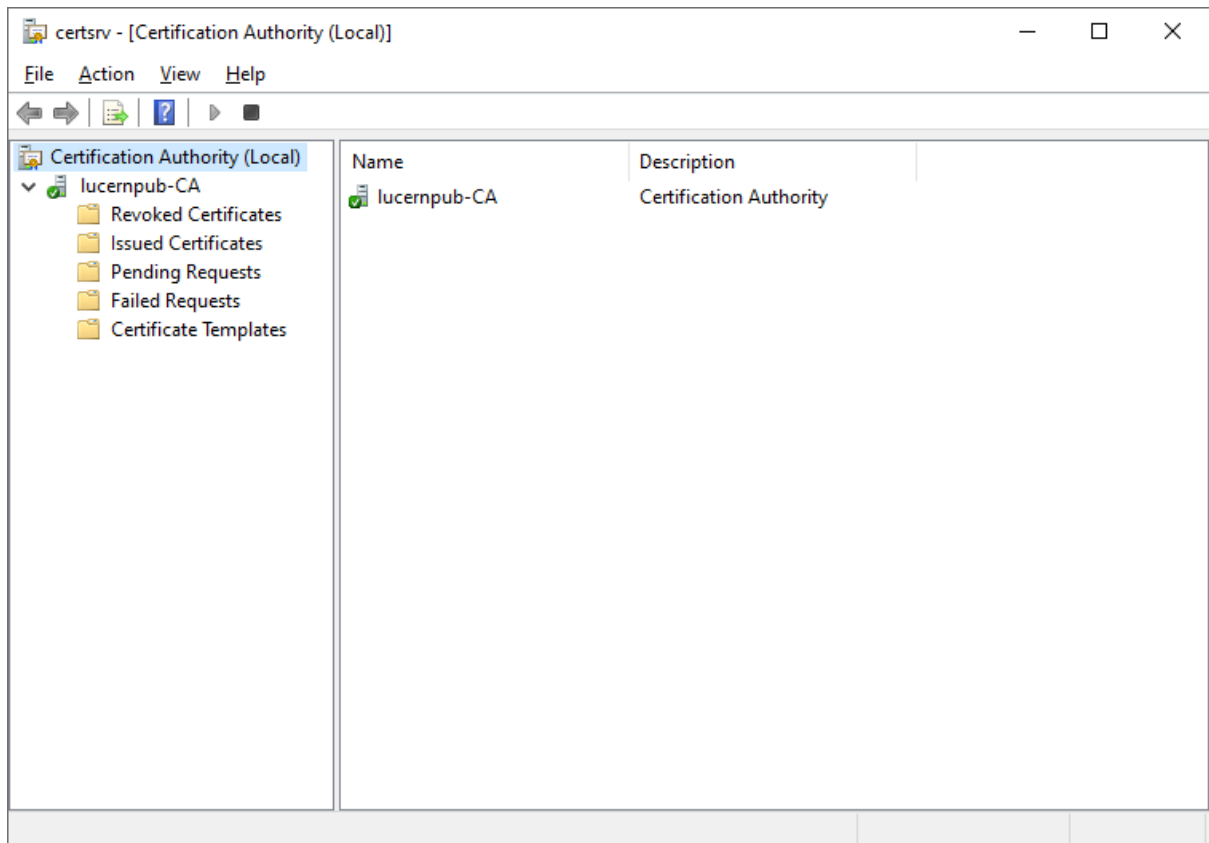
Roles	Description
<input checked="" type="checkbox"/> Active Directory Certificate Services (1 of 6 installed) <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Certification Authority (Installed) <input type="checkbox"/> Certificate Enrollment Policy Web Service <input type="checkbox"/> Certificate Enrollment Web Service <input type="checkbox"/> Certification Authority Web Enrollment <input type="checkbox"/> Network Device Enrollment Service <input checked="" type="checkbox"/> Online Responder 	Online Responder makes certificate revocation checking data accessible to clients in complex network environments.
<input type="checkbox"/> Active Directory Domain Services <input type="checkbox"/> Active Directory Federation Services <input type="checkbox"/> Active Directory Lightweight Directory Services <input type="checkbox"/> Active Directory Rights Management Services <input type="checkbox"/> Device Health Attestation <input type="checkbox"/> DHCP Server <input type="checkbox"/> DNS Server <input type="checkbox"/> Fax Server <input checked="" type="checkbox"/> File and Storage Services (2 of 12 installed) <ul style="list-style-type: none"> <input type="checkbox"/> Host Guardian Service <input type="checkbox"/> Hyper-V <input type="checkbox"/> Network Controller 	

< Previous

Next >


Install

Cancel




— □ ×



 Certificate Enrollment

Select Certificate Enrollment Policy

Certificate enrollment policy enables enrollment for certificates based on predefined certificate templates. Certificate enrollment policy may already be configured for you.

Configured by your administrator	
Active Directory Enrollment Policy	
Configured by you	
Add New	

Certificate Properties [X]

Subject | General | Extensions | Private Key | Certification Authority

The subject of a certificate is the user or computer to which the certificate is issued. You can enter information about the types of subject name and alternative name values that can be used in a certificate.

Subject of certificate
The user or computer that is receiving the certificate

Subject name:

Type: Common name [v]
Value: []

Add > < Remove

Alternative name:

Type: DNS [v]
Value: []

Add > < Remove

CN=adfs.lucernpub.com

DNS
adfs.lucernpub.com
enterpriseregistration.lucernpub.com
certauth.adfs.lucernpub.com

OK Cancel Apply

Properties of New Template [X]

Subject Name | Server | Issuance Requirements
Superseded Templates | Extensions | Security
Compatibility | General | Request Handling | Cryptography | Key Attestation

The template options available are based on the earliest operating system versions set in Compatibility Settings.

☒ Show resulting changes

Compatibility Settings

Certification Authority
Windows Server 2003 [v]

Certificate recipient
Windows XP / Server 2003 [v]

These settings may not prevent earlier operating systems from using this template.

OK Cancel Apply Help

Properties of New Template

Superseded Templates Extensions Security

Compatibility General Request Handling Cryptography Key Attestation

Subject Name Server Issuance Requirements

☐ Supply in the request

☐ Use subject information from existing certificates for autoenrollment renewal requests

☒ Build from this Active Directory information:

Select this option to enforce consistency among subject names and to simplify certificate administration.

Subject name format:

None

☐ Include e-mail name in subject name

Include this information in alternate subject name:

☐ E-mail name

☒ DNS name

☐ User principal name (UPN)

☐ Service principal name (SPN)

OK Cancel Apply Help

Properties of New Template

Compatibility General Request Handling Cryptography Key Attestation

Subject Name Server Issuance Requirements

Superseded Templates Extensions Security

Add Superseded Template

Select one or more certificate templates to add to the list of superseded templates.

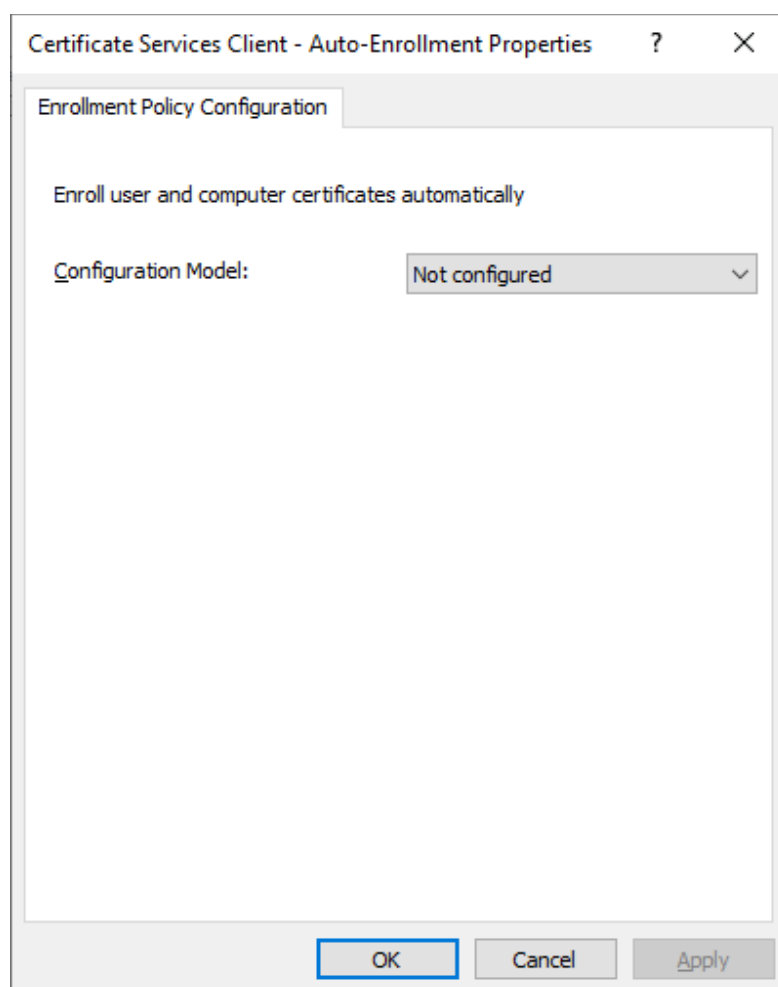
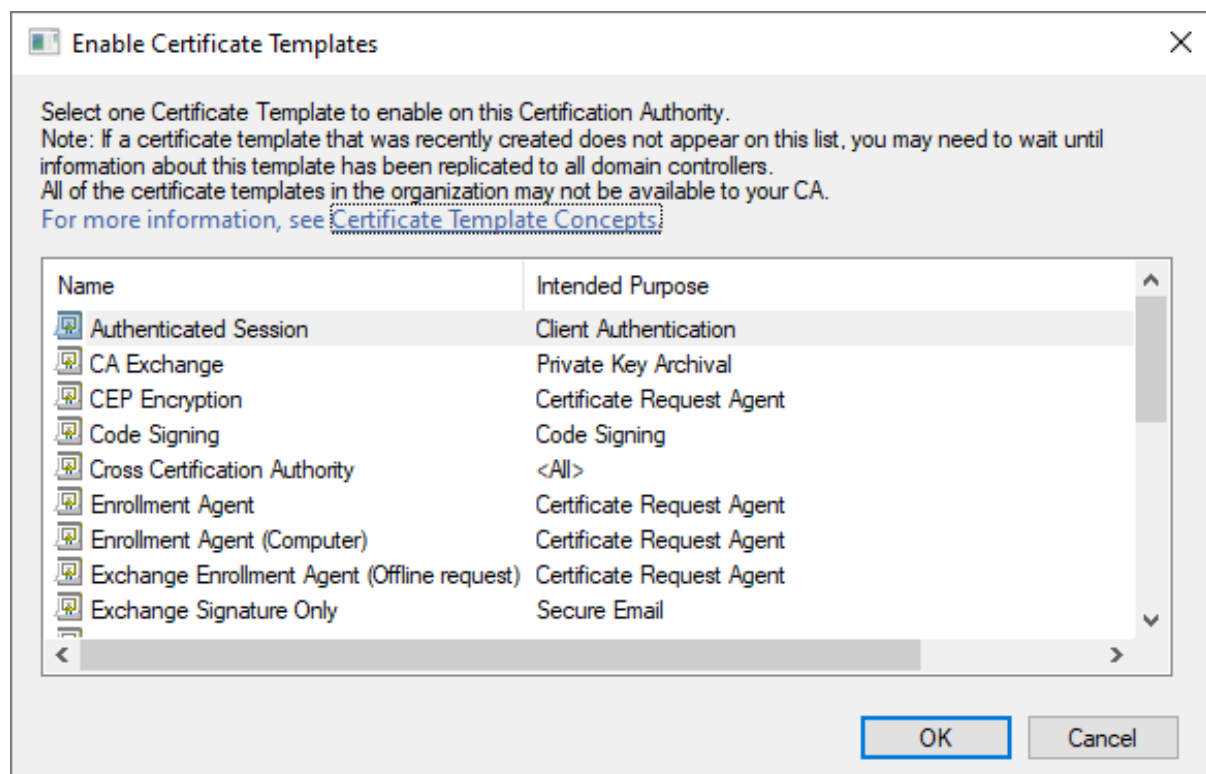
Certificate templates:

Template Display Name	Minimum Supported CAs
Administrator	Windows 2000
Authenticated Session	Windows 2000
Basic EFS	Windows 2000
CA Exchange	Windows Server 2003 Ente
CEP Encryption	Windows 2000
Code Signing	Windows 2000
Computer	Windows 2000
Directory Email Replication	Windows Server 2003 Ente
Domain Controller	Windows 2000

Properties...

OK Cancel

OK Cancel Apply Help



Certificate Revocation



Are you sure you want to revoke the selected certificate(s)?

Specify a reason, date and time.

Readon code:

Unspecified

Date and Time:

9/ 4/2021


9:33 AM

Yes

No

Chapter 13: Managing Federation

Windows Server version	WID scale limit
Windows Server 2008	5 AD FS servers
Windows Server 2008 Release 2 (R2)	
Windows Server 2012	
Windows Server 2012 R2	
Windows Server 2016	30 AD FS servers
Windows Server 2019	
Windows Server 2022	

 Add Roles and Features Wizard

Active Directory Federation Services (AD FS)

Before You Begin

Installation Type

Server Selection

Server Roles

Features

AD FS


Confirmation

Results

Active Directory Federation Services (AD FS) provides Web single-sign-on (SSO) capabilities to authenticate a user to multiple Web applications using a single user account. AD FS helps organizations bypass the need for secondary accounts by allowing you to project a user's digital identity and access rights to trusted partners. In this federated environment, each organization continues to manage its own identities.

Things to note:

- This computer must be joined to a domain before you can successfully install the Federation Service.
- The Web Application Proxy role service in the Remote Access server role functions as the federation service proxy and cannot be installed on the same computer as the federation service.



Azure Active Directory, a separate online service, can provide simplified identity and access management, security reporting, single sign-on to cloud and on-premises web apps.

[Learn more about Azure Active Directory](#)

[Configure Office 365 with Azure Active Directory Connect](#)

< Previous

Next >

Install

Cancel

Specify Service Properties

Welcome

Connect to AD DS

Specify Service Properties

Specify Service Account

Specify Database

Review Options

Pre-requisite Checks

Installation

Results

SSL Certificate:

Import...

View

Federation Service Name:

Example: fs.contoso.com

Federation Service Display Name: *

Users will see the display name at sign in.

Example: Contoso Corporation

< Previous

Next >

Configure

Cancel

Specify Service Account

Welcome

Connect to AD DS

Specify Service Properties

Specify Service Account

Specify Database

Review Options

Pre-requisite Checks

Installation

Results

Specify a domain user account or group Managed Service Account.

☒ Create a Group Managed Service Account

Account Name:

LUCERNPUB*

☐ Use an existing domain user account or group Managed Service Account

Account Name:

<Not provided>

Select...

< Previous

Next >

Configure

Cancel

Welcome

Welcome

Connect to AD DS

Specify Farm

Specify Certificate

Specify Service Account

Review Options

Pre-requisite Checks

Installation

Results

Welcome to the Active Directory Federation Services Configuration Wizard.

Before you begin configuration, you must have the following:

- An Active Directory domain administrator account.
- A publicly trusted certificate for SSL server authentication.

AD FS prerequisites

Select an option below:

☐ Create the first federation server in a federation server farm

☒ Add a federation server to a federation server farm

Configuring sign-in to Office 365? Exit this wizard and use Azure Active Directory Connect.

[Learn more about Azure Active Directory Connect.](#)

< Previous

Next >

Configure

Cancel

Remove server roles

DESTINATION SERVER
ADFS01.lucernpub.com

Before You Begin

Server Selection

Server Roles

Features

Confirmation

Results

To remove one or more installed roles from the selected server, clear their check boxes.

Roles

- ☐ Active Directory Certificate Services (Not installed)
- ☐ Active Directory Domain Services (Not installed)
- ☒ Active Directory Federation Services
- ☐ Active Directory Lightweight Directory Services (Not installed)
- ☐ Active Directory Rights Management Services (Not installed)
- ☐ Device Health Attestation (Not installed)
- ☐ DHCP Server (Not installed)
- ☐ DNS Server (Not installed)
- ☐ Fax Server (Not installed)
- ☒ File and Storage Services
- ☐ Host Guardian Service (Not installed)
- ☐ Hyper-V (Not installed)
- ☐ Network Controller (Not installed)
- ☐ Network Policy and Access Services (Not installed)
- ☐ Print and Document Services (Not installed)
- ☐ Remote Access (Not installed)
- ☐ Remote Desktop Services (Not installed)
- ☐ Volume Activation Services (Not installed)
- ☐ Web Server (IIS) (Not installed)

Description

Active Directory Certificate Services (AD CS) is used to create certification authorities and related role services that allow you to issue and manage certificates used in a variety of applications.

< Previous

Next >

Remove

Cancel

Welcome**Steps**

- Welcome
- Select Data Source
- Choose Access Control Policy
- Ready to Add Trust
- Finish

Welcome to the Add Relying Party Trust Wizard

Claims-aware applications consume claims in security tokens to make authentication and authorization decisions. Non-claims-aware applications are web-based and use Windows Integrated Authentication in the internal network and can be published through Web Application Proxy for extranet access. [Learn more](#)

- ☒ Claims aware
- ☐ Non claims aware

< Previous

Start

Cancel

Configure Rule**Steps**

- Choose Rule Type
- Configure Claim Rule

You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.

Claim rule name:

Rule template: Send LDAP Attributes as Claims

Attribute store:

Select an attribute store... ▾

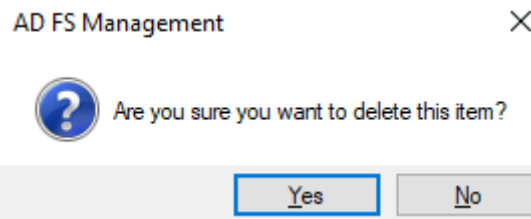
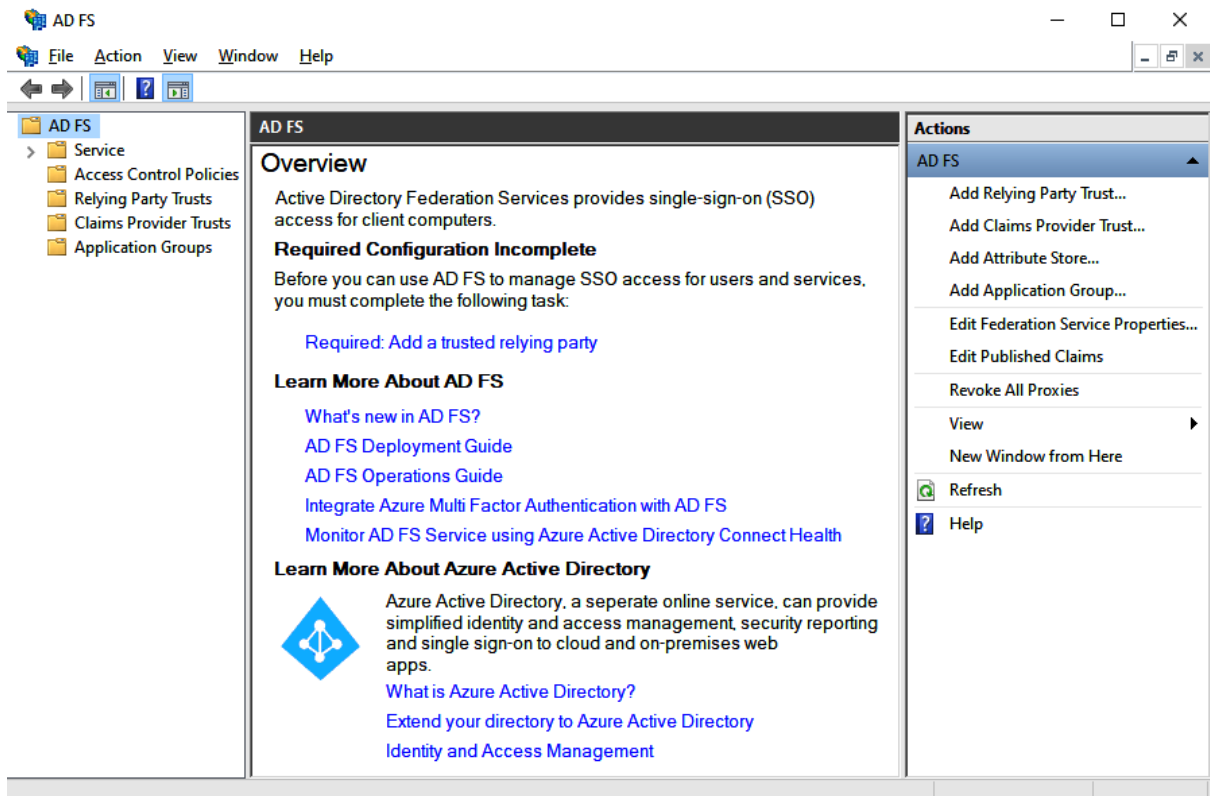
Mapping of LDAP attributes to outgoing claim types:

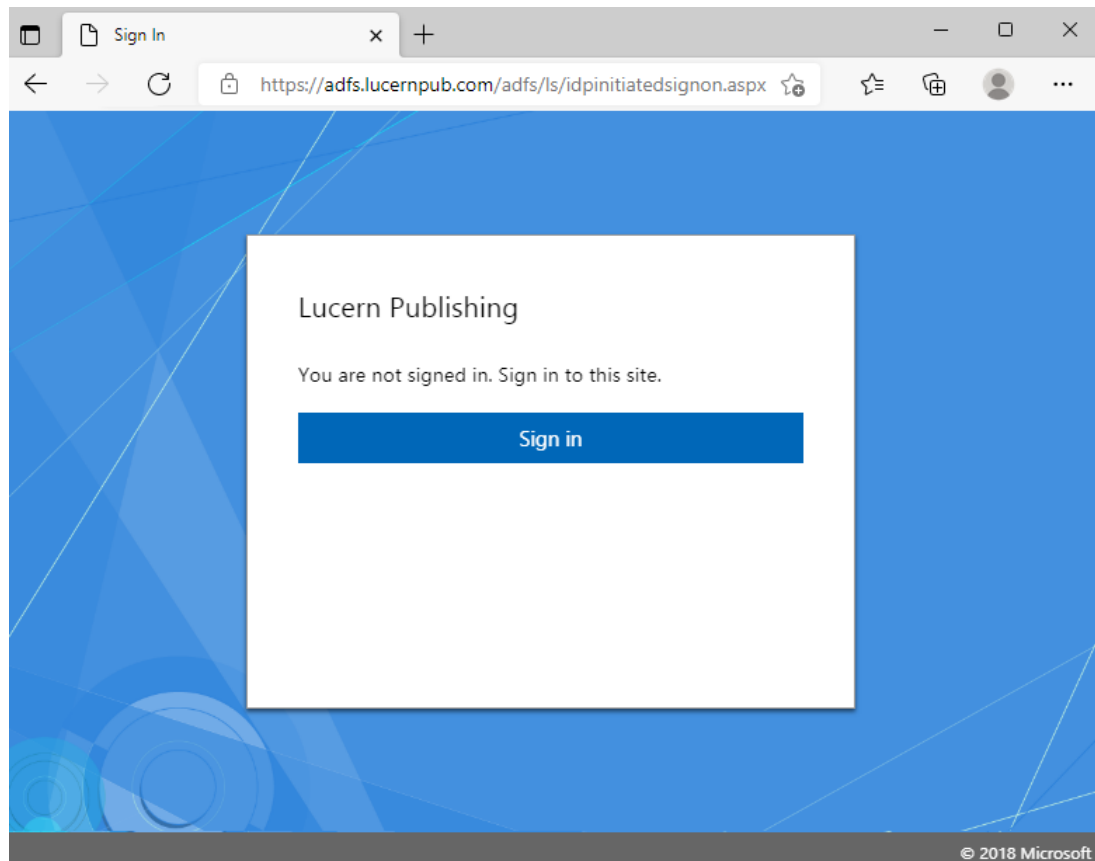
	LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
*	<input type="text"/>	<input type="text"/>

< Previous

Finish

Cancel





Add Roles and Features Wizard

Select role services

Before You Begin

Installation Type

Server Selection

Server Roles

Features

Remote Access

Role Services

Confirmation

Results

Select the role services to install for Remote Access

Role services

- ☐ DirectAccess and VPN (RAS)
- ☐ Routing
- ☐ Web Application Proxy

Description

Web Application Proxy enables the publishing of selected HTTP- and HTTPS-based applications from your corporate network to client devices outside of the corporate network. It can use AD FS to ensure that users are authenticated before they gain access to published applications. Web Application Proxy also provides proxy functionality for your AD FS servers.

< Previous

Next >

Install

Cancel

Federation Server

Welcome

Federation Server

AD FS Proxy Certificate

Confirmation

Results

Select the Active Directory Federation Services (AD FS) server to use for Web Application Proxy authentication and authorization.

Federation service name:

Enter the credentials of a local administrator account on the federation servers.

User name:

Password:

< Previous

Next >

Configure

Cancel

Confirm removal selections

Before You Begin

Server Selection

Server Roles

Features

Confirmation

Results

To remove the following roles, role services, or features from the selected server, click Remove.

☐ Restart the destination server automatically if required

Group Policy Management

RAS Connection Manager Administration Kit (CMAC)

Remote Access

Web Application Proxy

Remote Server Administration Tools

Role Administration Tools

Remote Access Management Tools

Remote Access GUI and Command-Line Tools

Remote Access module for Windows PowerShell

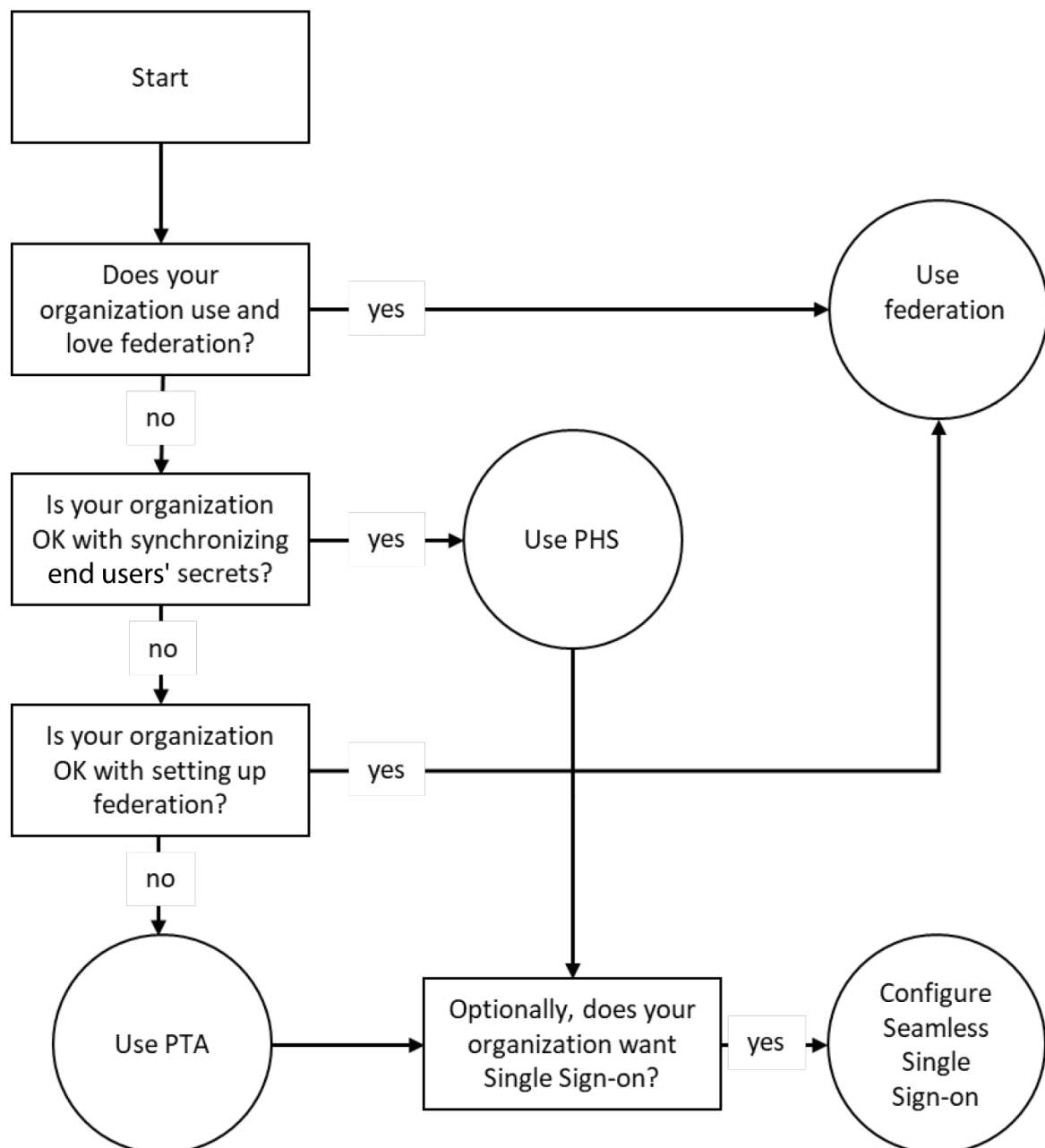
< Previous

Next >

Remove

Cancel

Chapter 14: Handling Authentication in a Hybrid World (AD FS, PHS, PTA, and DSSO)



Lucern Publishing - Azure Active Directory admin center

https://aad.portal.azure.com/#blade/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/Domains

Azure Active Directory admin center

Dashboard > Lucern Publishing

Lucern Publishing | Custom domain names

Azure Active Directory

+ Add custom domain Refresh Troubleshoot Columns Got feedback?

Looking to move an on-premises application to the cloud and use Azure Active Directory Domain Services?

Search domains Add filters

Name	Status	Federated	Primary
.onmicrosoft.com	Available		✓

Overview

Preview features

Diagnose and solve problems

Manage

- Users
- Groups
- External identities
- Roles and administrators
- Administrative units
- Enterprise applications
- Devices
- App registrations
- Identity Governance
- Application proxy
- Custom security attributes (Preview)
- Licenses
- Azure AD Connect
- Custom domain names

Microsoft Azure Active Directory Connect

Welcome

Express Settings

Express Settings

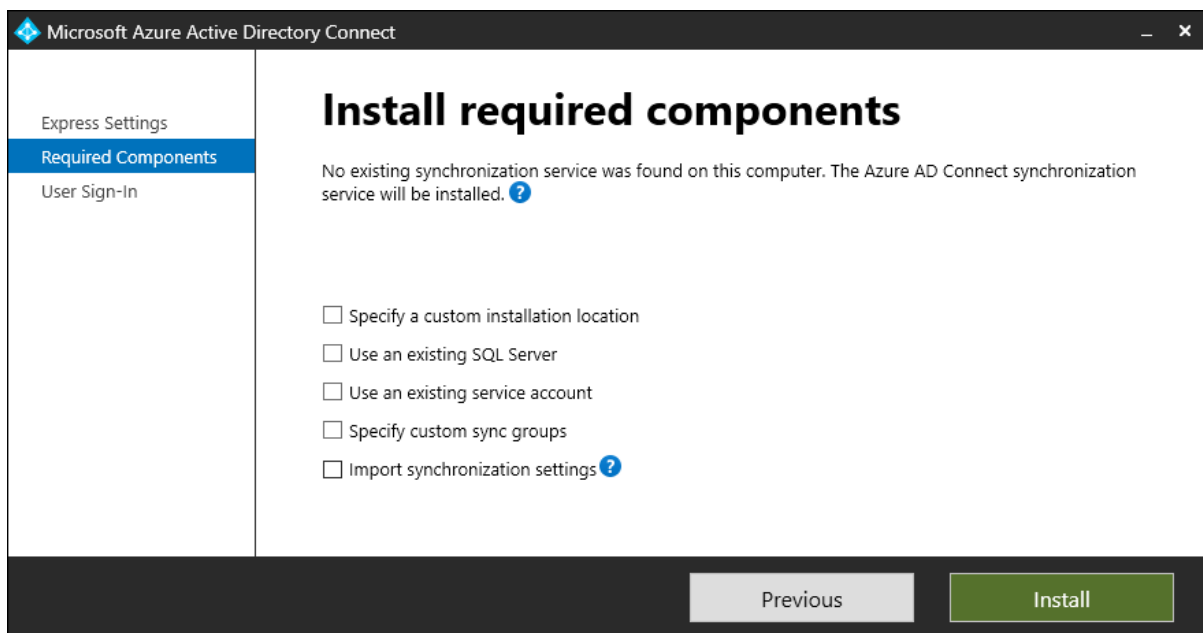
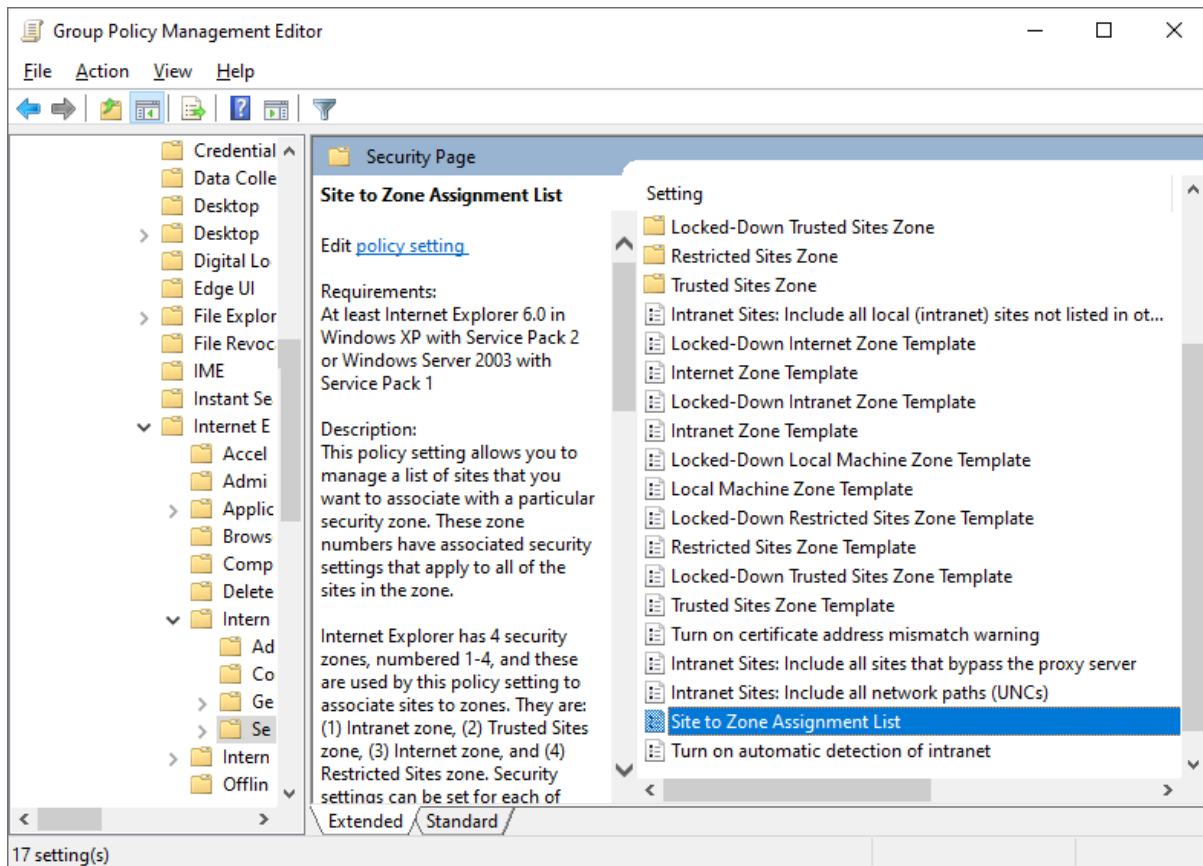
If you have a **single** Windows Server Active Directory forest, we will do the following:

- Configure synchronization of identities in the current AD forest of **LUCERNPUB**
- Configure password hash synchronization from on-premises AD to Azure AD
- Start an initial synchronization
- Synchronize all attributes
- Enable Auto Upgrade

[Learn more about express settings](#)

Select Customize to choose advanced deployment options or import settings from an existing server.

Customize Use express settings



Microsoft Azure Active Directory Connect

Express Settings
Required Components
User Sign-In
Connect to Azure AD
Sync
Connect Directories
Azure AD sign-in
Domain/OU Filtering
Identifying users
Filtering
Optional Features
Single sign-on
Configure

Connect your directories

Enter connection information for your on-premises directories or forests. ?

DIRECTORY TYPE

Active Directory

FOREST ?

Add Directory

No directories are currently configured.

PreviousNext

Microsoft Azure Active Directory Connect

Express Settings
Required Components
User Sign-In
Connect to Azure AD
Sync
Connect Directories
Azure AD sign-in
Domain/OU Filtering
Identifying users
Filtering
Optional Features
Single sign-on
Configure

Ready to configure

Once you click Install, we will do the following:

- Configure synchronization services on this computer
- Install Microsoft Azure AD Connect Authentication Agent for Pass-Through Authentication
- Enable Pass-through authentication
- Enable single sign-on
- Configure Source Anchor Attribute
- Configure lucerndemo21.onmicrosoft.com - AAD Connector
- Configure lucernpub.com Connector
- Disable Password hash synchronization

☒ Start the synchronization process when configuration completes.

☐ Enable staging mode: When selected, synchronization will not export any data to AD or Azure AD.

PreviousInstall

Microsoft Azure Active Directory Connect

Express Settings

Required Components

User Sign-In

Connect to Azure AD

Sync

Connect Directories

Azure AD sign-in

Domain/OU Filtering

Identifying users

Filtering

Optional Features

Credentials

AD FS Farm

Azure AD domain

Configure

Verify connectivity

AD forest account

AD forest account

An AD account with sufficient permissions is required for periodic synchronization. Azure AD Connect can create the account for you. Alternatively, you may provide an existing account with the required permissions. [Learn more](#) about managing account permissions.

The first option is recommended and requires you to enter Enterprise Admin credentials.

Select account option.

☒ Create new AD account

☐ Use existing AD account

ENTERPRISE ADMIN USERNAME

PASSWORD

OK

Cancel

Previous

Next

Microsoft Azure Active Directory Connect

Express Settings

Required Components

User Sign-In

Connect to Azure AD

Sync

Connect Directories

Azure AD sign-in

Domain/OU Filtering

Identifying users

Filtering

Optional Features

Credentials

AD FS Farm

Federation server

Proxy server

Service account

Azure AD domain

Configure

Verify connectivity

AD FS farm

Configure a new AD FS farm

Use an existing AD FS farm

Provide a password-protected PFX file containing the SSL certificate that will be used to secure the communication between clients and AD FS.

CERTIFICATE FILE ?

Browse

AAD Connect will store the PFX file locally. Ensure that a strong password has been used to protect the certificate.

Previous

Next

Microsoft Azure Active Directory Connect

Express Settings
Required Components
User Sign-In
Connect to Azure AD
Sync
 Connect Directories
 Azure AD sign-in
 Domain/OU Filtering
 Identifying users
 Filtering
 Optional Features
Credentials
AD FS Farm
 Federation server
 Proxy server
Service account
Azure AD domain
Configure
Verify connectivity

AD FS service account

Specify the AD FS service log on account. ?

Create a group Managed Service Account

Use an existing group Managed Service Account

Use a domain user account

Previous

Next

Microsoft Azure Active Directory Connect

Welcome
Tasks
Manage federation

Manage federation

The following tasks are available for managing your federation service. Choose from the list below to perform additional tasks.

View federation configuration ?

Federate Azure AD domain ?

Manage Azure AD trust ?

Manage certificates ?

Manage servers ?

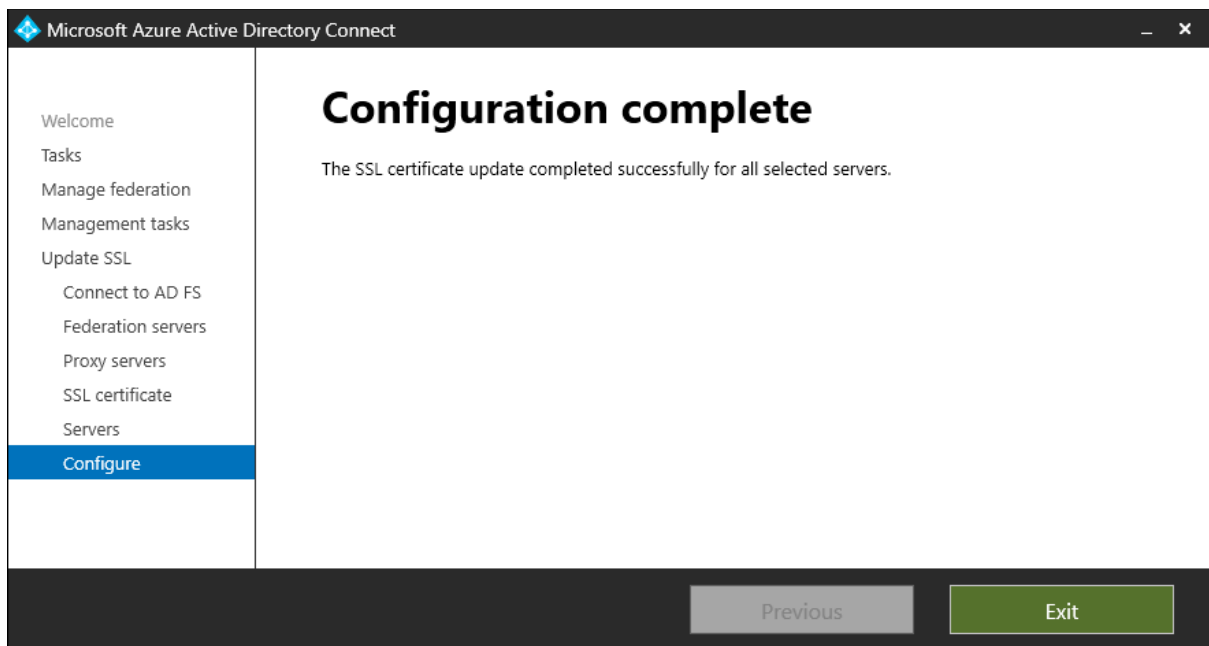
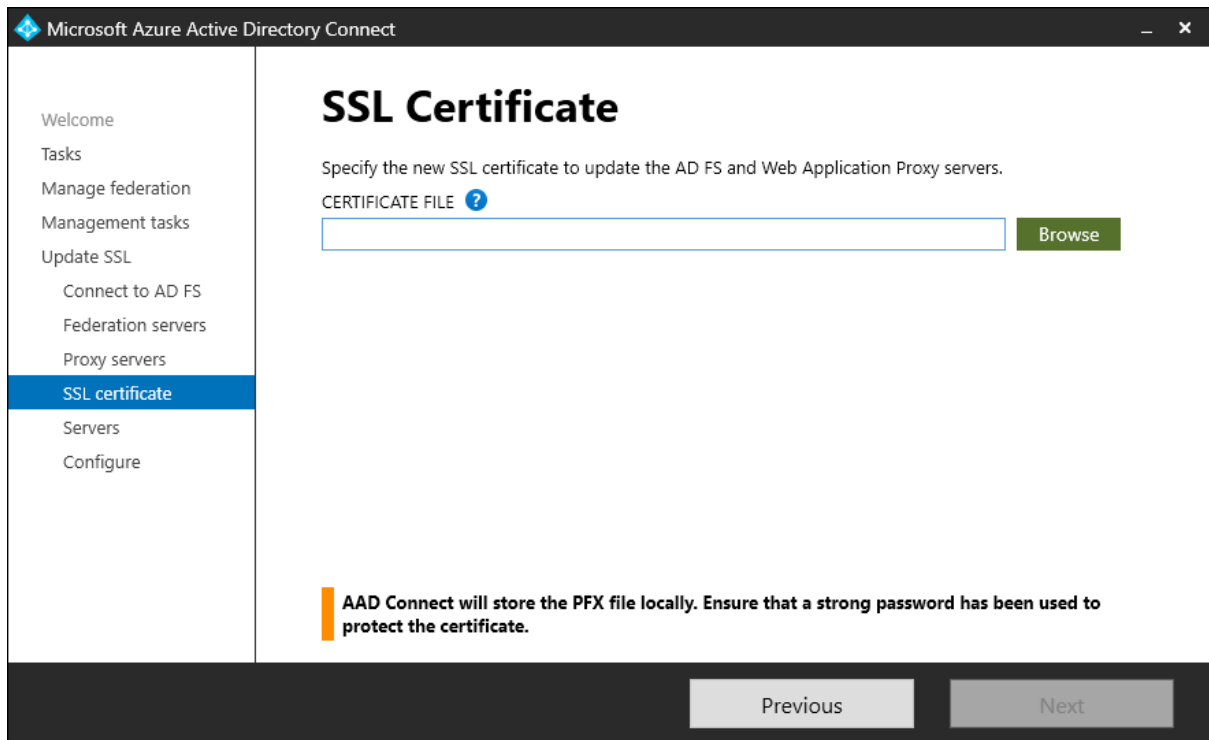
Verify federated login ?

Verify federation connectivity ?

The AD FS Help website provides multiple online tools, troubleshooting guides, and links to open source projects that can be used for managing your federation service. [AD FS Help](#)

Previous

Next



Microsoft Azure Active Directory Connect

Welcome

Tasks

Manage federation

Management tasks

Deploy AD FS server

Connect to AD FS

SSL certificate

Federation server

Configure

Verify connectivity

Specify SSL certificate

To install Active Directory Federation Services, an SSL certificate is required to identify your organization. The certificate must match the identity of the federation service.

CERTIFICATE FILE ?

SSL certificate already provided

Browse

Provide the password for the previously provided certificate.

ENTER PASSWORD

Previous

Next

LucernSTS - Microsoft Azure

https://portal.azure.com

Microsoft Azure

Search resources, services, and docs (G+/)

Dashboard >

LucernSTS

Traffic Manager profile

Search (Ctrl+/)

Enable profile

Disable profile

Refresh

JSON View

Essentials

Resource group [\(move\)](#)

[LucernPub](#)

Status

Enabled

Subscription [\(move\)](#)

Subscription ID

DNS name

http://lucernsts.trafficmanager.net

Monitor status

Inactive

Routing method

Performance

Tags [\(edit\)](#)

[Click here to add tags](#)

Search endpoints

Name	↑↓	Status	↑↓	Monitor status	↑↓
No results.					

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Configuration

Real user measurements

Traffic view

Endpoints

Properties

Locks

Monitoring

Alerts

Metrics

Diagnostic settings

Logs

Automation

Tasks (preview)

Microsoft Azure Active Directory Connect

WelcomeTasksConnect to Azure ADUser Sign-InSingle sign-onConfigure

User sign-in

Select the Sign On method. ?

☐ Password Hash Synchronization ?

☐ Warning: Your Azure AD domains will be converted from federated to managed authentication. Confirm this by selecting the checkbox. [Learn more](#)

☒ Pass-through authentication ?

☐ Warning: Your Azure AD domains will be converted from federated to managed authentication. Confirm this by selecting the checkbox. [Learn more](#)

☐ Federation with AD FS ?

☐ Federation with PingFederate ?

☐ Do not configure ?

Select this option to enable single sign-on for your corporate desktop users:

☒ Enable single sign-on ?

Previous

Next

Microsoft Azure Active Directory Connect

WelcomeTasksConnect to Azure ADUser Sign-InSingle sign-onConfigure

Ready to configure

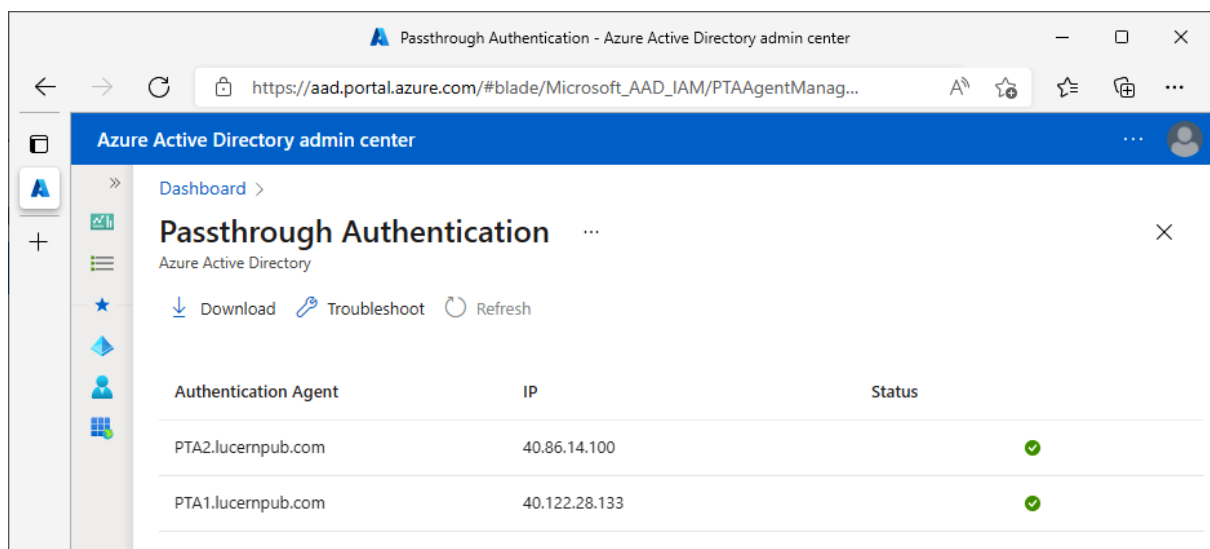
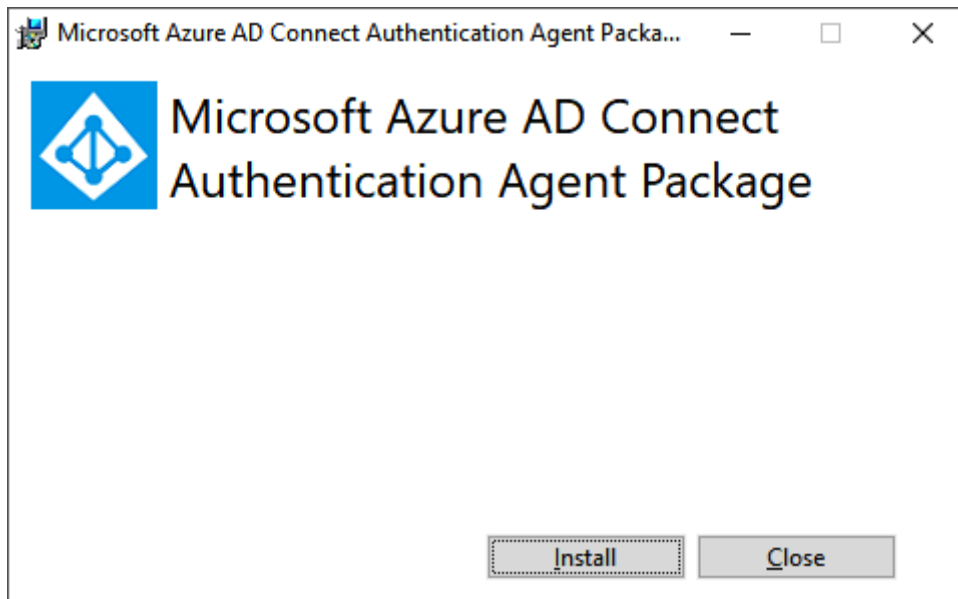
Once you click Configure, we will do the following:

- Install Microsoft Azure AD Connect Authentication Agent for Pass-Through Authentication
- Enable Pass-through authentication
- Enable managed authentication in Azure
- Enable single sign-on

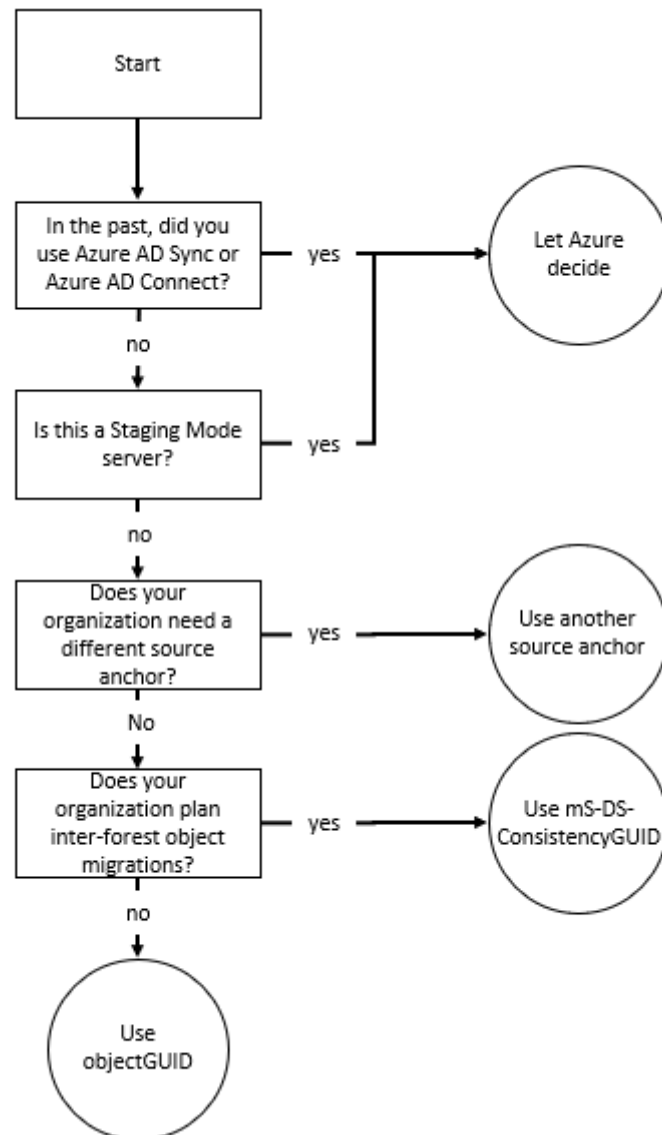
☒ Start the synchronization process when configuration completes.

Previous

Configure



Chapter 15: Handling Synchronization in a Hybrid World (Azure AD Connect)



Microsoft Azure Active Directory Connect

WelcomeExpress SettingsRequired ComponentsUser Sign-InConnect to Azure ADSyncConnect DirectoriesAzure AD sign-inDomain/OU FilteringIdentifying usersFilteringOptional FeaturesCredentialsAD FS FarmAzure AD domainConfigureVerify connectivity

Uniquely identifying your users

Select how users should be identified in your on-premises directories. ?

☒ Users are represented only once across all directories.

☐ User identities exist across multiple directories. Match using:

☒ Mail attribute

☐ ObjectSID and msExchMasterAccountSID/msRTCSIP-OriginatorSID attributes

☐ SAMAccountName and MailNickName attributes

☐ A specific attribute

Select how users should be identified with Azure AD. ?

☒ Let Azure manage the source anchor

☐ Choose a specific attribute

Azure is currently synchronized using mS-DS-ConsistencyGuid and will write back the source anchor for your on-premises users. [Learn more](#)

Previous

Next

Microsoft Azure Active Directory Connect

WelcomeTasks

Additional tasks

The required tasks for the scenario have been completed. Choose from the list below to perform additional tasks.

Privacy settings

View or export current configuration

Customize synchronization options

Configure device options ?

Refresh directory schema

Configure staging mode

Change user sign-in

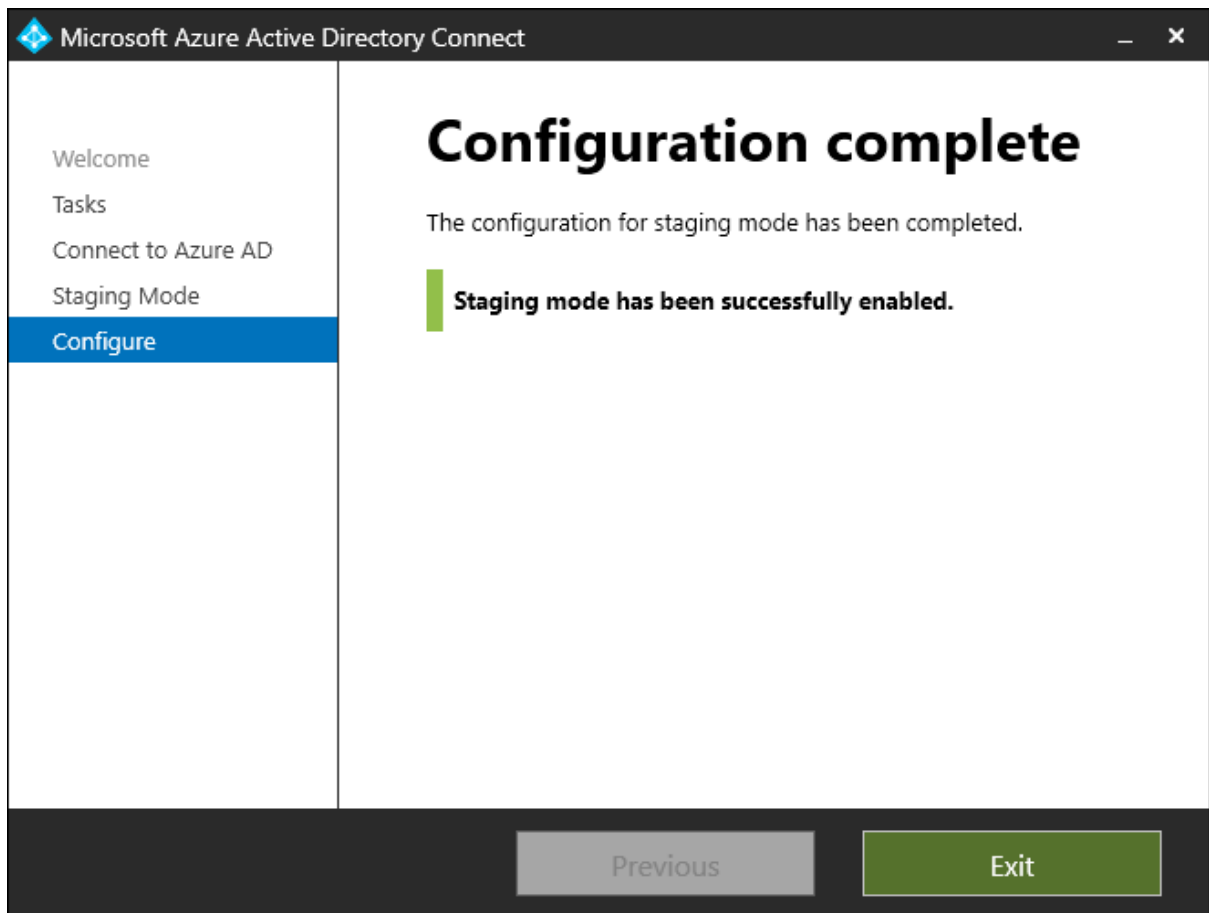
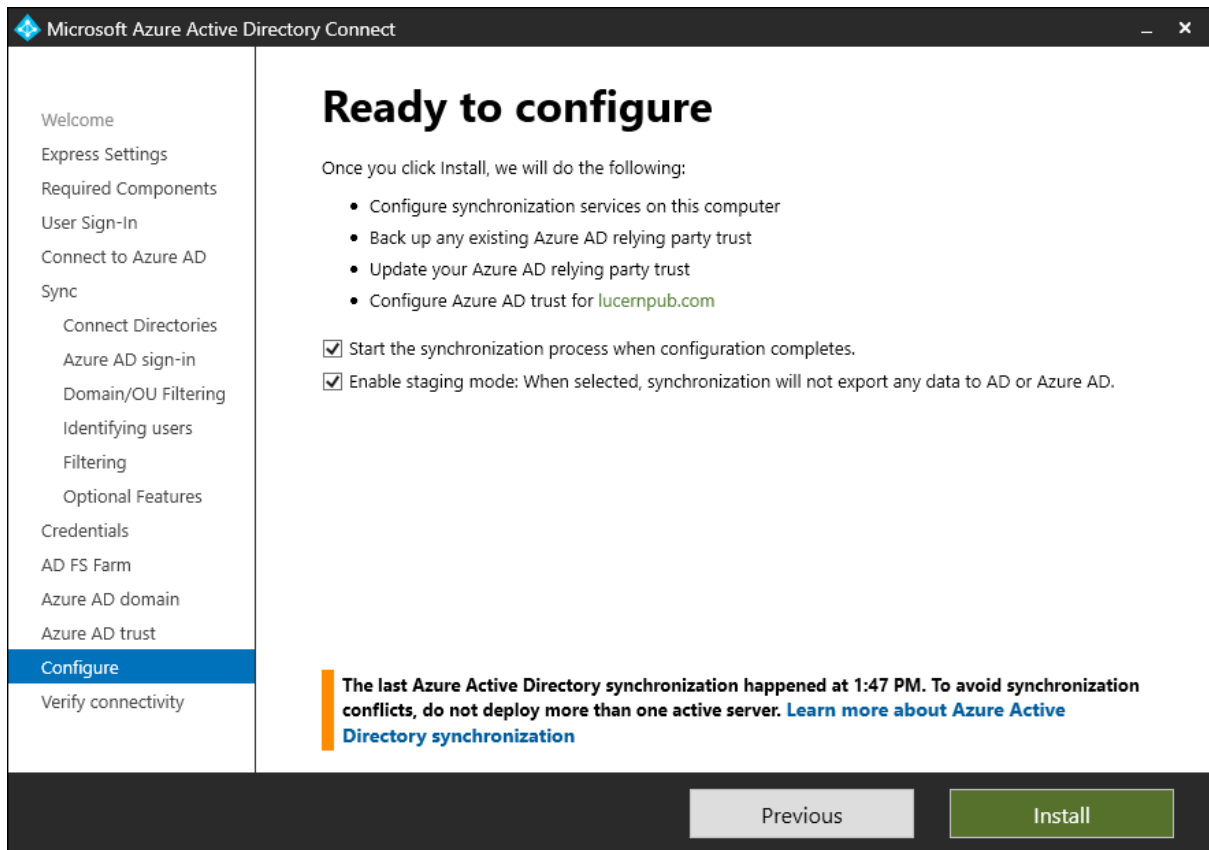
Configure Source Anchor

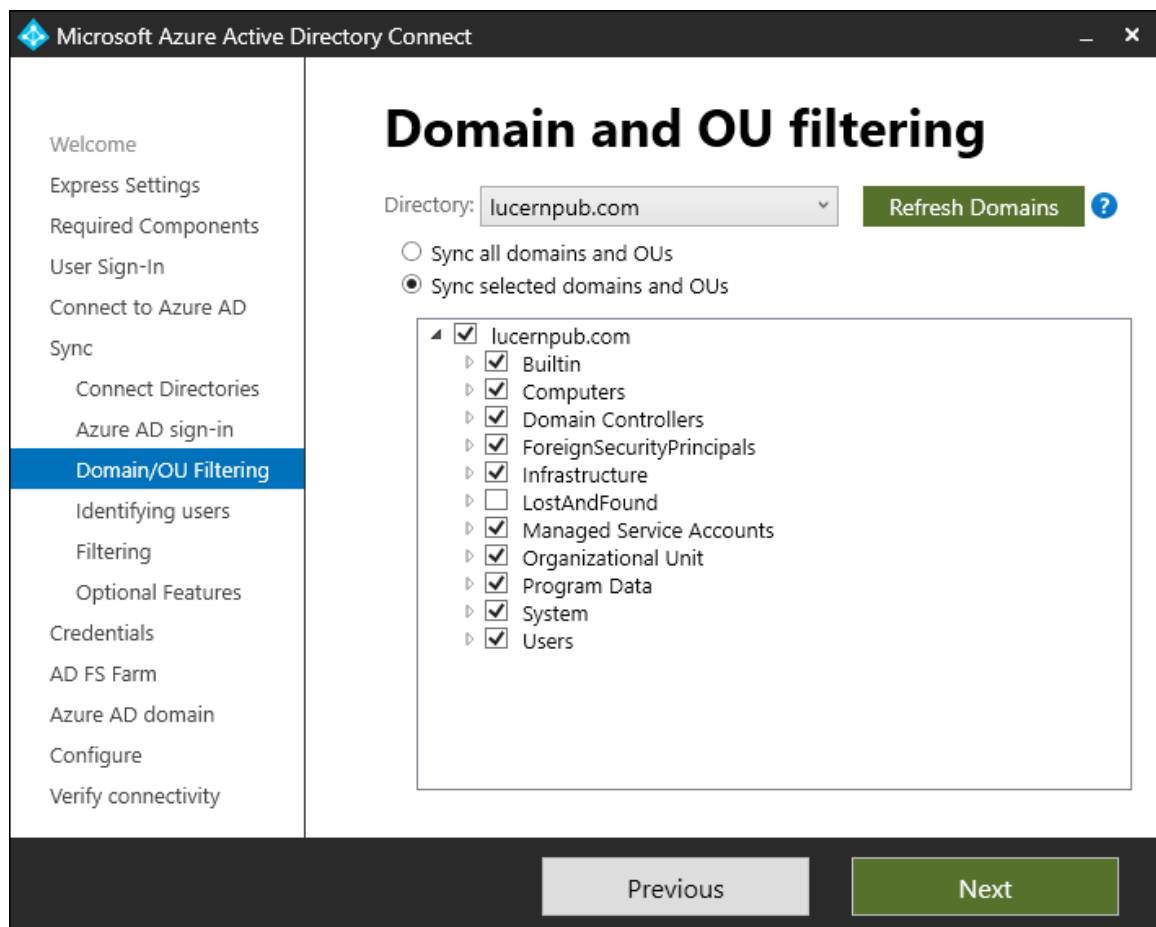
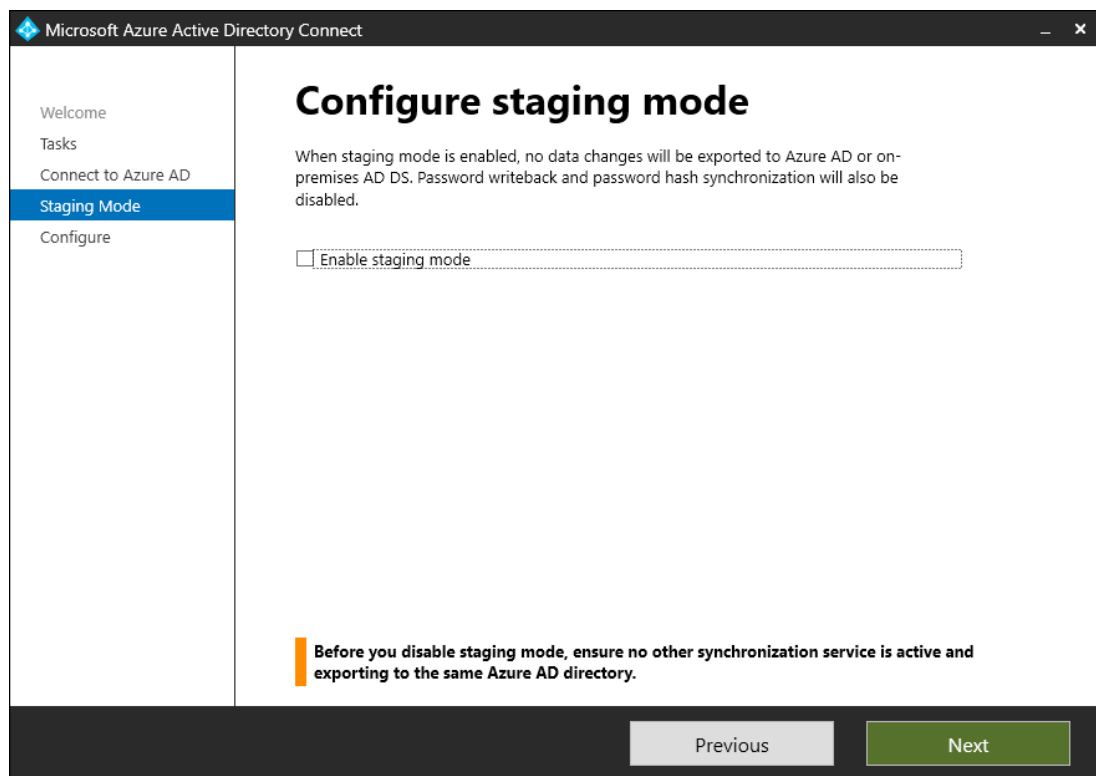
Manage federation ?

Troubleshoot

Previous

Next





Microsoft Azure Active Directory Connect

Welcome

Tasks

Additional tasks

The required tasks for the scenario have been completed. Choose from the list below to perform additional tasks.

Privacy settings

View or export current configuration

Customize synchronization options

Configure device options ?

Refresh directory schema

Configure staging mode

Change user sign-in

Configure Source Anchor

Manage federation ?

Troubleshoot

Previous

Next

Microsoft Azure Active Directory Connect

Welcome

Express Settings

Required Components

User Sign-In

Connect to Azure AD

Sync

Connect Directories

Azure AD sign-in

Domain/OU Filtering

Identifying users

Filtering

Optional Features

Azure AD Apps

Azure AD Attributes

Credentials

AD FS Farm

Azure AD domain

Configure

Verify connectivity

Optional features

Select enhanced functionality if required by your organization.

☐ Exchange hybrid deployment ?

☐ Exchange Mail Public Folders ?

☒ Azure AD app and attribute filtering ?

☐ Password hash synchronization ?

☐ Password writeback ?

☐ Group writeback ?

☐ Device writeback ?

☐ Directory extension attribute sync ?

[Learn more](#) about optional features.

Previous

Next

Microsoft Azure Active Directory Connect

Welcome
Tasks
Connect to Azure AD
Sync
Connect Directories
Domain/OU Filtering
Optional Features
Azure AD Apps
Azure AD Attributes
Configure

Azure AD apps

The information necessary to use the following apps will be exported to Azure AD. Remove an app only if required to meet strict organizational security policy.

AZURE AD APPS

- ☒ Office 365 ProPlus
- ☒ Exchange Online
- ☒ SharePoint Online
- ☒ Lync Online
- ☒ Azure RMS
- ☒ Intune
- ☒ Dynamics CRM
- ☒ 3rd party application

☐ I want to restrict the list of applications. ?

Previous
Next

Site to Zone Assignment List

Site to Zone Assignment List

Previous Setting
Next Setting

☒ Not Configured
☐ Enabled
☐ Disabled

Comment:

Supported on:

At least Internet Explorer 6.0 in Windows XP with Service Pack 2 or Windows Server 2003 with Service Pack 1

Options:

Enter the zone assignments here.
Show...

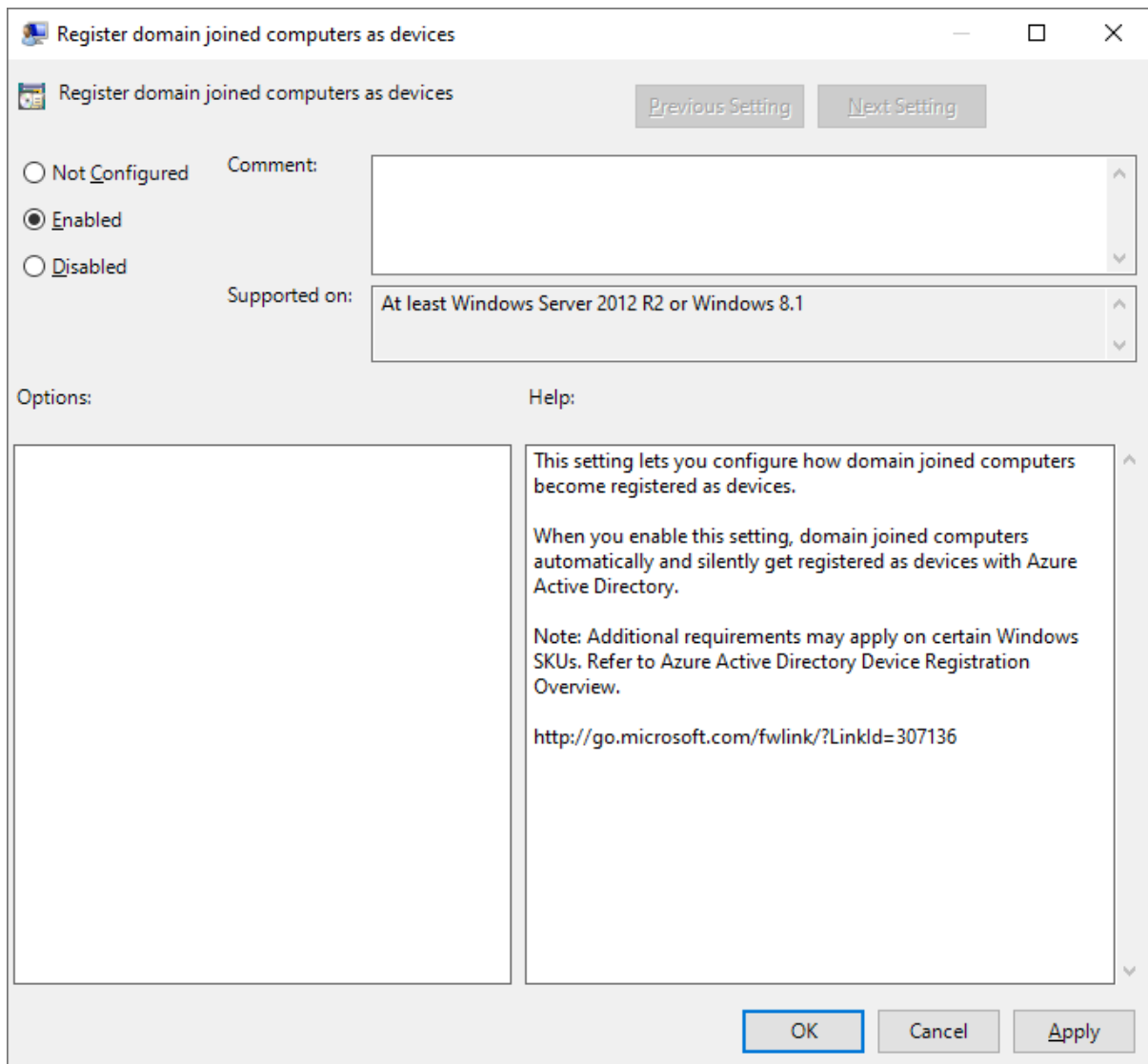
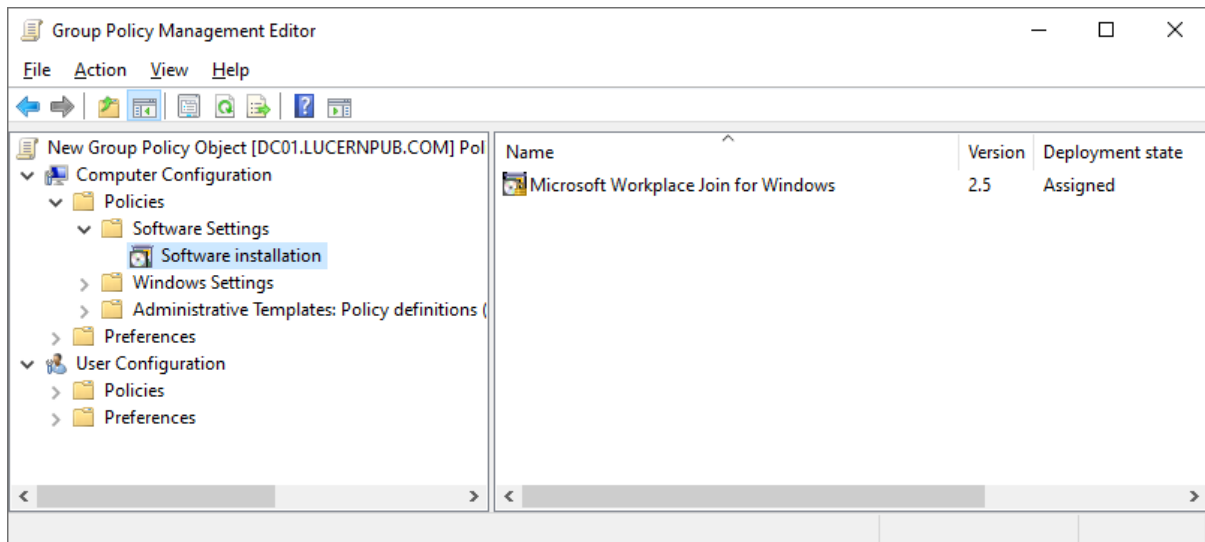
Help:

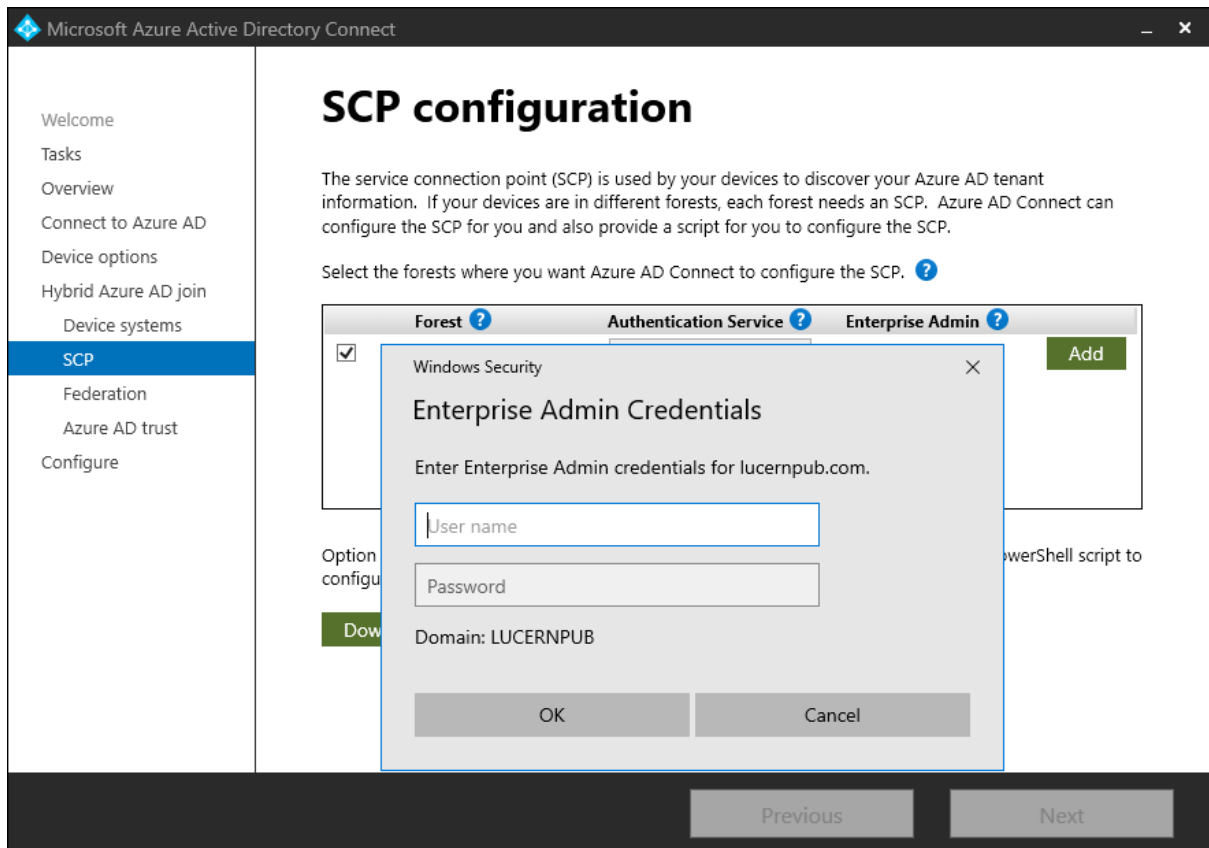
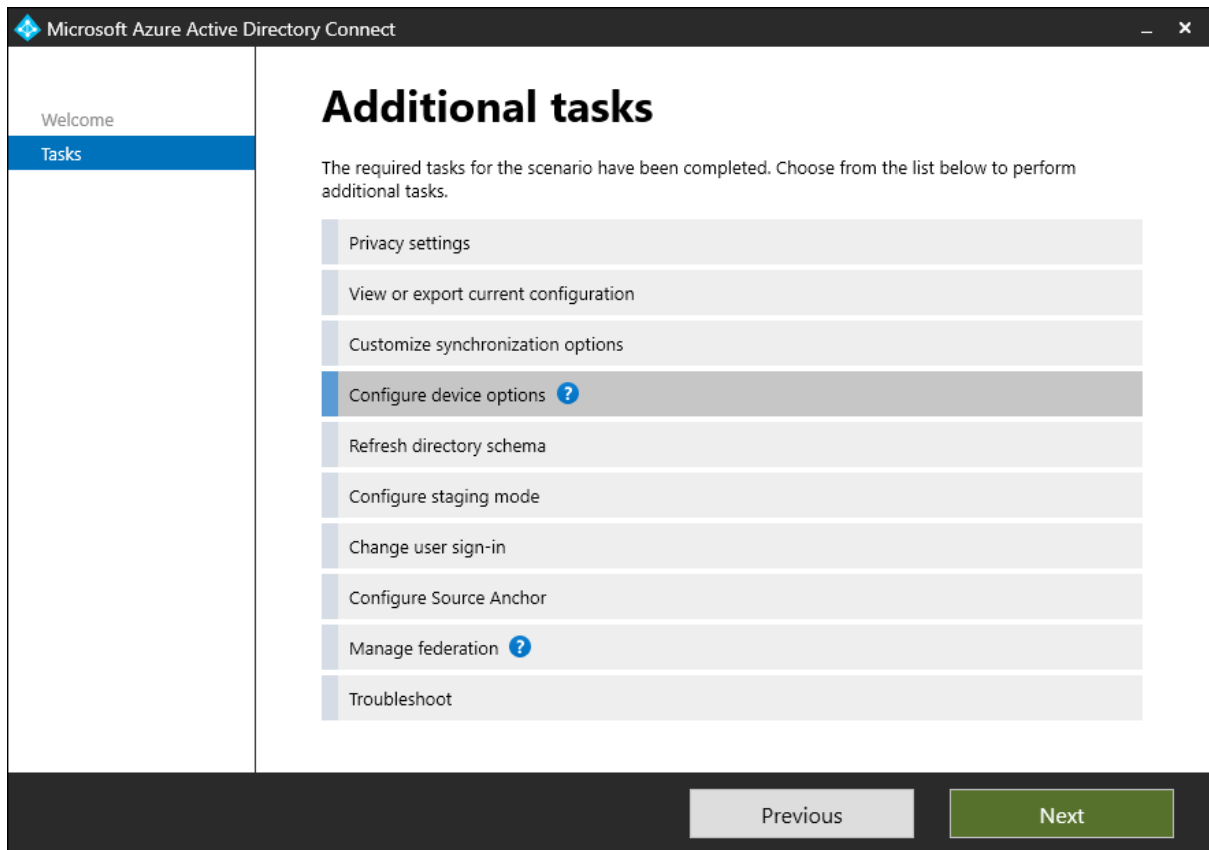
This policy setting allows you to manage a list of sites that you want to associate with a particular security zone. These zone numbers have associated security settings that apply to all of the sites in the zone.

Internet Explorer has 4 security zones, numbered 1-4, and these are used by this policy setting to associate sites to zones. They are: (1) Intranet zone, (2) Trusted Sites zone, (3) Internet zone, and (4) Restricted Sites zone. Security settings can be set for each of these zones through other policy settings, and their default settings are: Trusted Sites zone (Low template), Intranet zone (Medium-Low template), Internet zone (Medium template), and Restricted Sites zone (High template). (The Local Machine zone and its locked down equivalent have special security settings that protect your local computer.)

If you enable this policy setting, you can enter a list of sites and their related zone numbers. The association of a site with a zone will ensure that the security settings for the specified zone are applied to the site. For each entry that you add to the list, enter the following information:

OK
Cancel
Apply





Microsoft Azure Active Directory Connect

WelcomeTasksOverviewConnect to Azure ADDevice optionsDevice writebackForestContainerConfigure

Writeback forest

Select the on-premises destination for device writeback from Azure AD. Azure AD Connect will create a device container object in the selected forest. Device objects will be synchronized to the selected domain.

Device writeback forest ?

Device writeback location ?

PreviousNext

Microsoft Azure Active Directory Connect

WelcomeExpress SettingsRequired ComponentsUser Sign-InConnect to Azure ADSyncConnect DirectoriesAzure AD sign-inDomain/OU FilteringIdentifying usersFilteringOptional FeaturesCredentialsAD FS FarmAzure AD domainConfigureVerify connectivity

Optional features

Select enhanced functionality if required by your organization.

☐ Exchange hybrid deployment ?☐ Exchange Mail Public Folders ?☐ Azure AD app and attribute filtering ?☐ Password hash synchronization ?☒ Password writeback ?☐ Group writeback ?☐ Device writeback ?☐ Directory extension attribute sync ?

[Learn more](#) about optional features.

PreviousNext

Microsoft Azure Active Directory Connect

WelcomeTasksConnect to Azure ADSyncConnect DirectoriesDomain/OU FilteringOptional FeaturesConfigure

Optional features

Select enhanced functionality if required by your organization.

☐ Exchange hybrid deployment ?☐ Exchange Mail Public Folders ?☐ Azure AD app and attribute filtering ?☐ Password hash synchronization ?☒ Password writeback ?☐ Group writeback ?☐ Device writeback ?☐ Directory extension attribute sync ?

[Learn more](#) about optional features.

PreviousNext

Microsoft Azure Active Directory Connect

WelcomeExpress SettingsRequired ComponentsUser Sign-InConnect to Azure ADSyncConnect DirectoriesAzure AD sign-inDomain/OU FilteringIdentifying usersFilteringOptional FeaturesGroup WritebackCredentialsAD FS FarmAzure AD domainConfigureVerify connectivity

Group Writeback

Select the on-premises destination for group writeback.

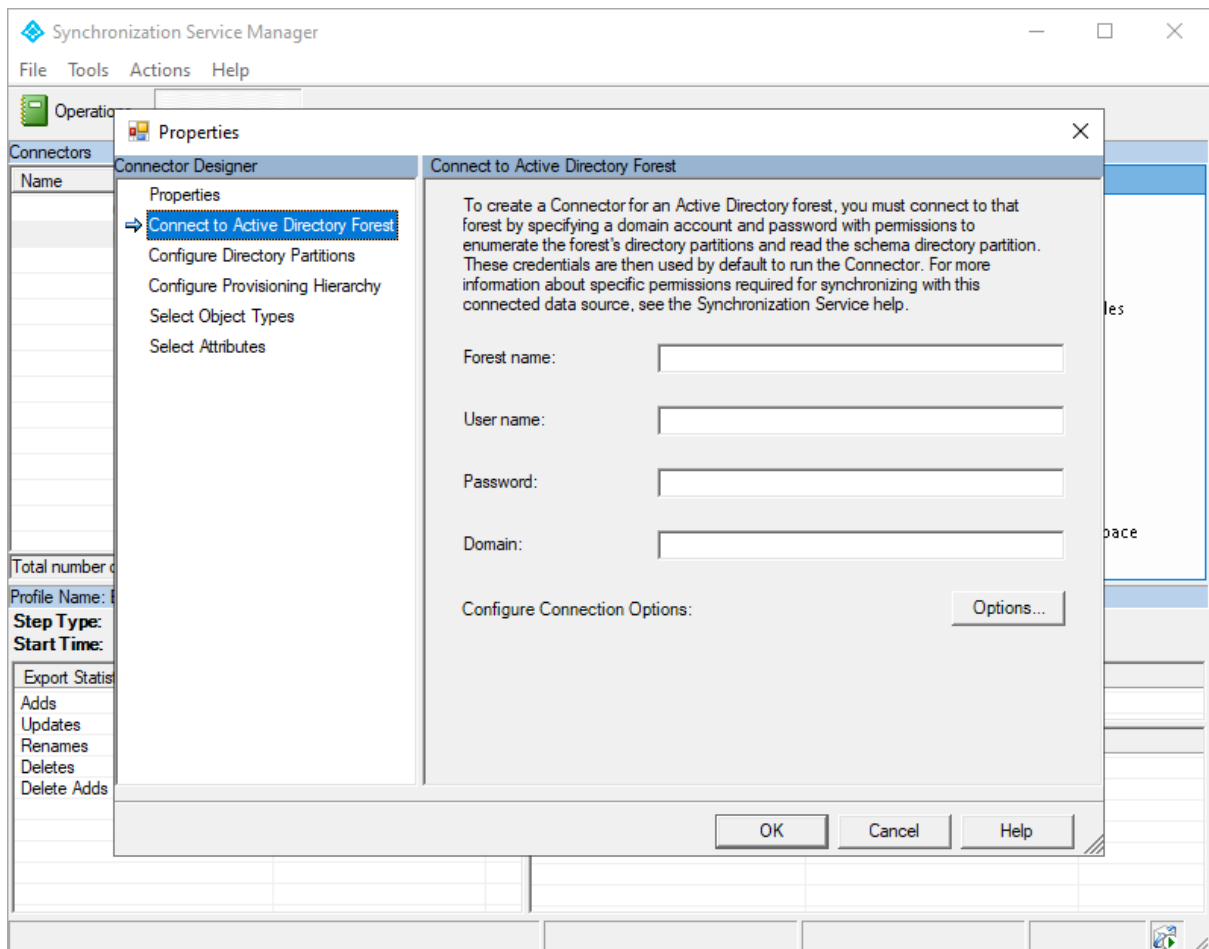
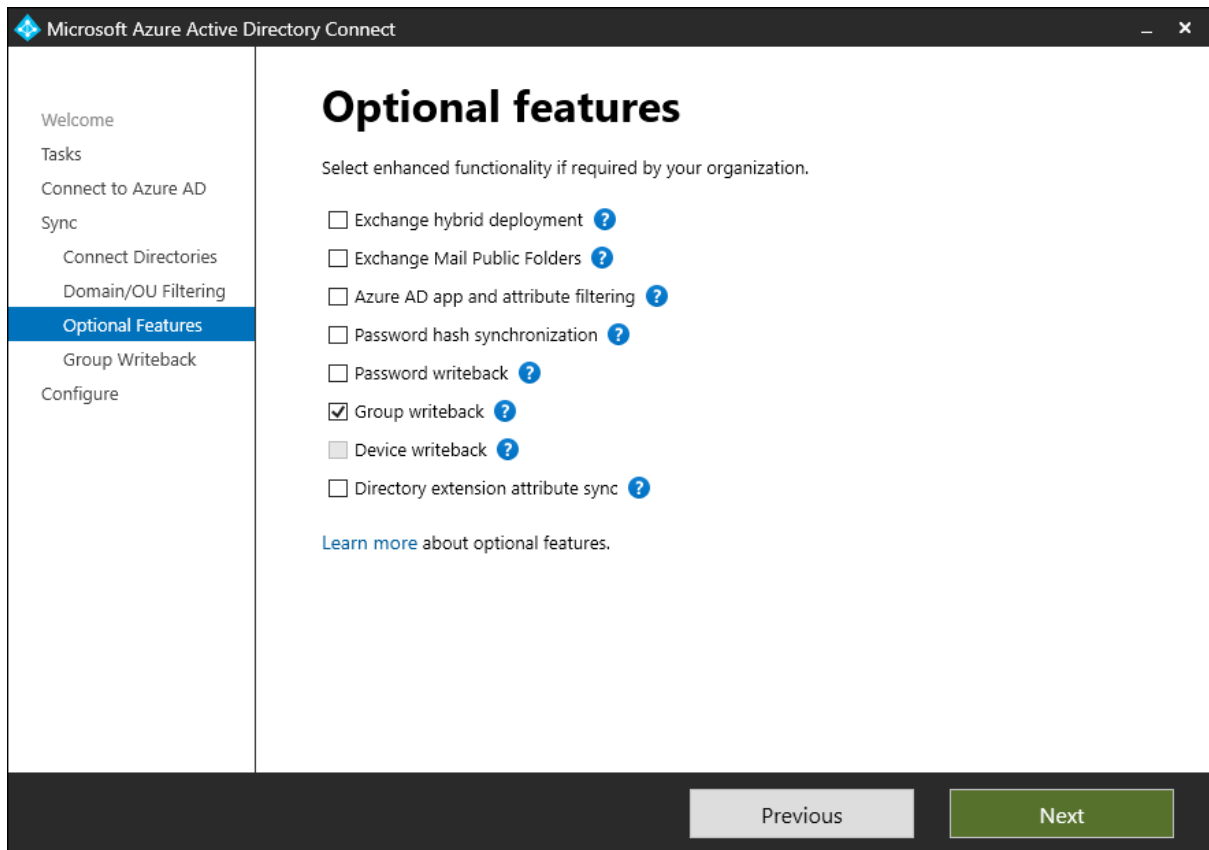
Group writeback forest ?

Group writeback destination ?

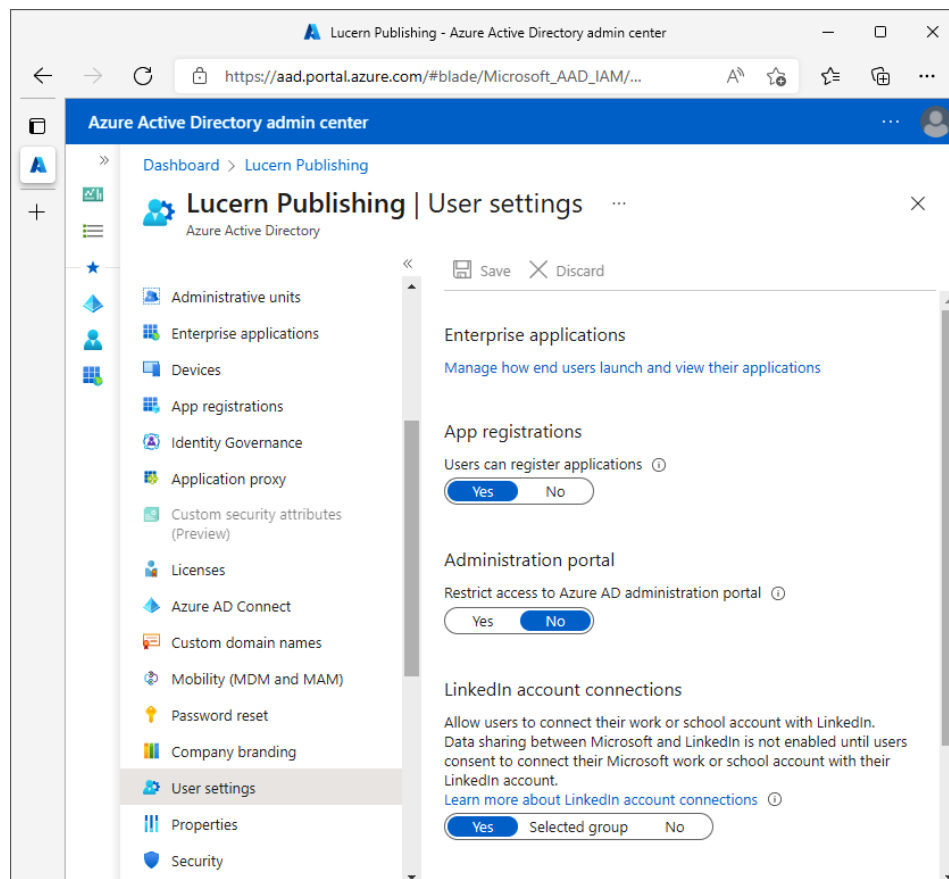
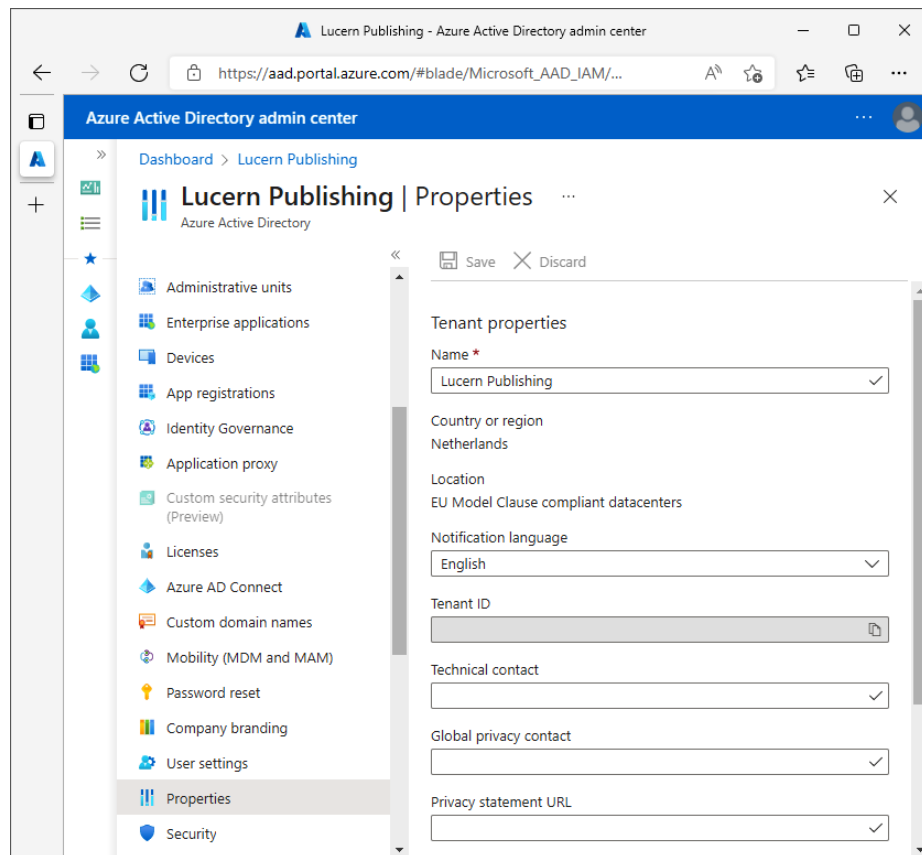
ComputersDomain ControllersForeignSecurityPrincipalsManaged Service AccountsOrganizational UnitProgram DataSystemUsers

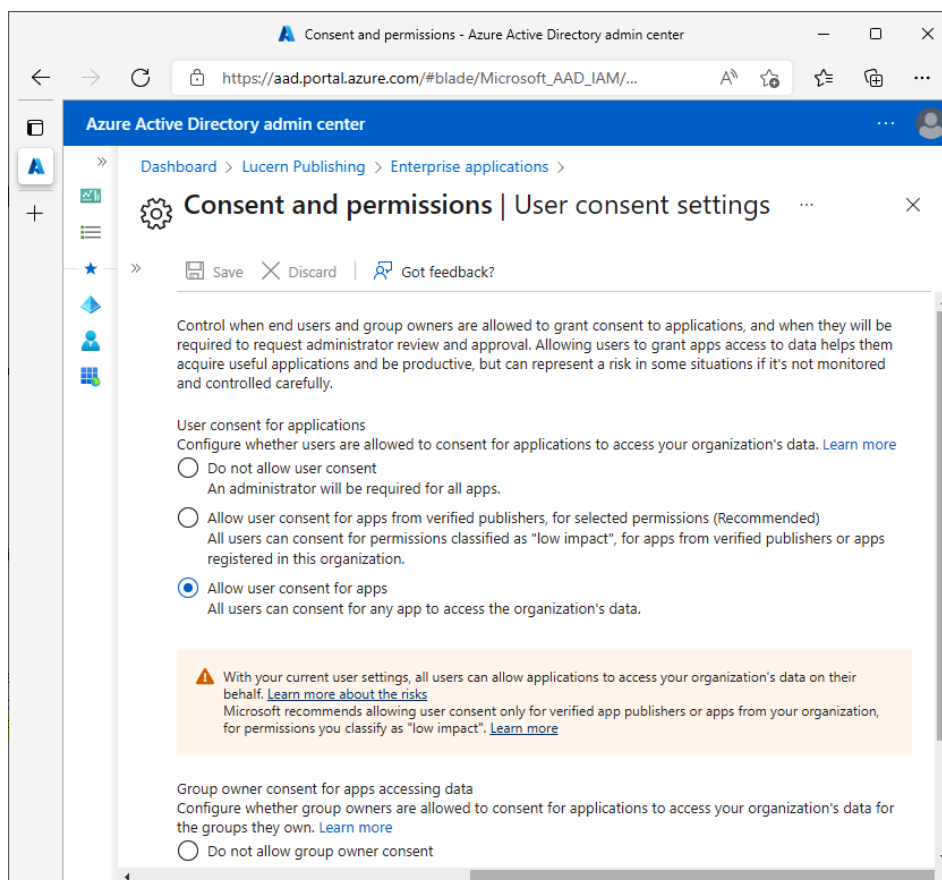
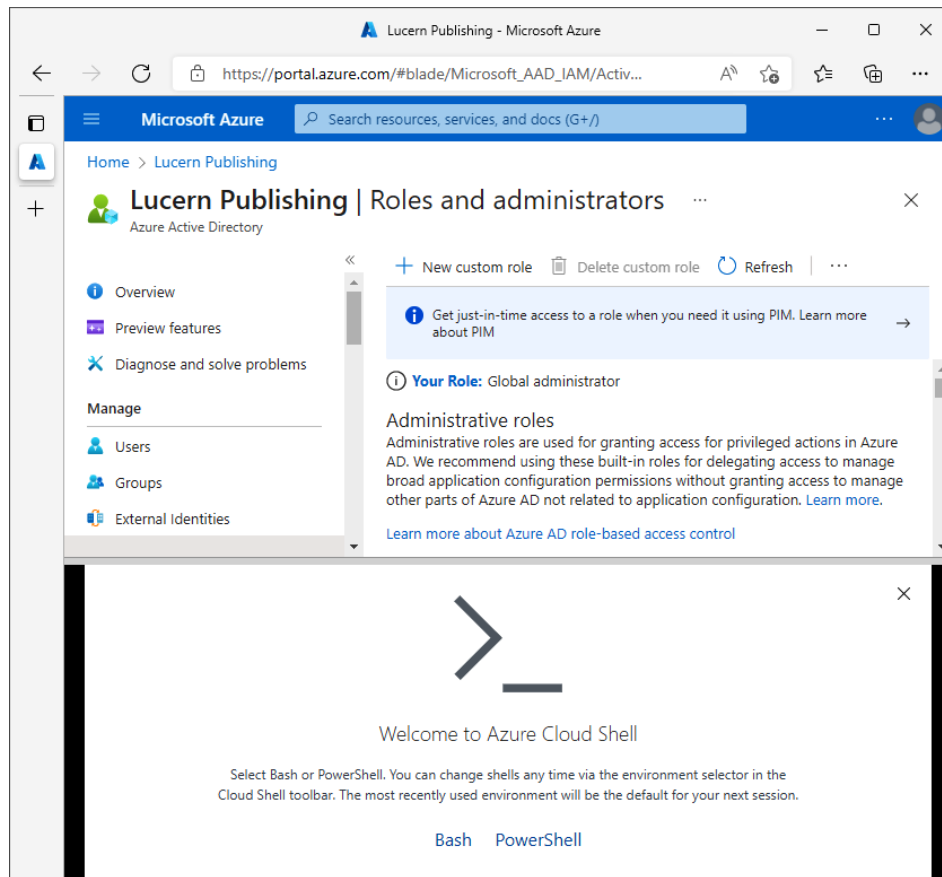
☒ Writeback Group Distinguished Name with cloud Display Name ?

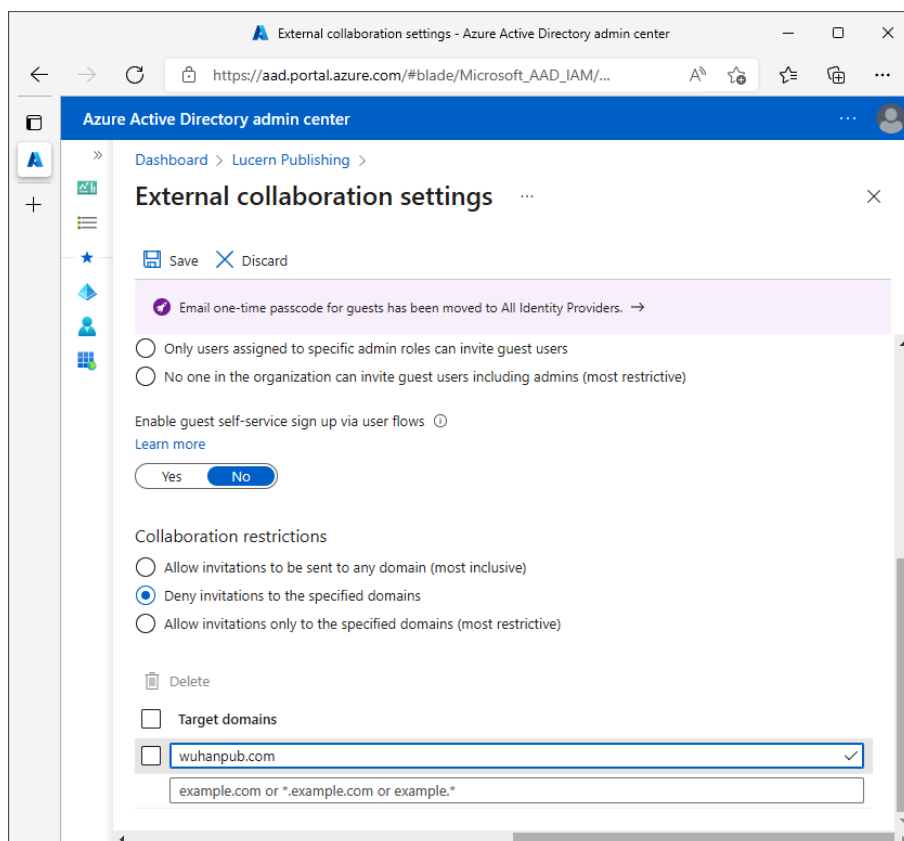
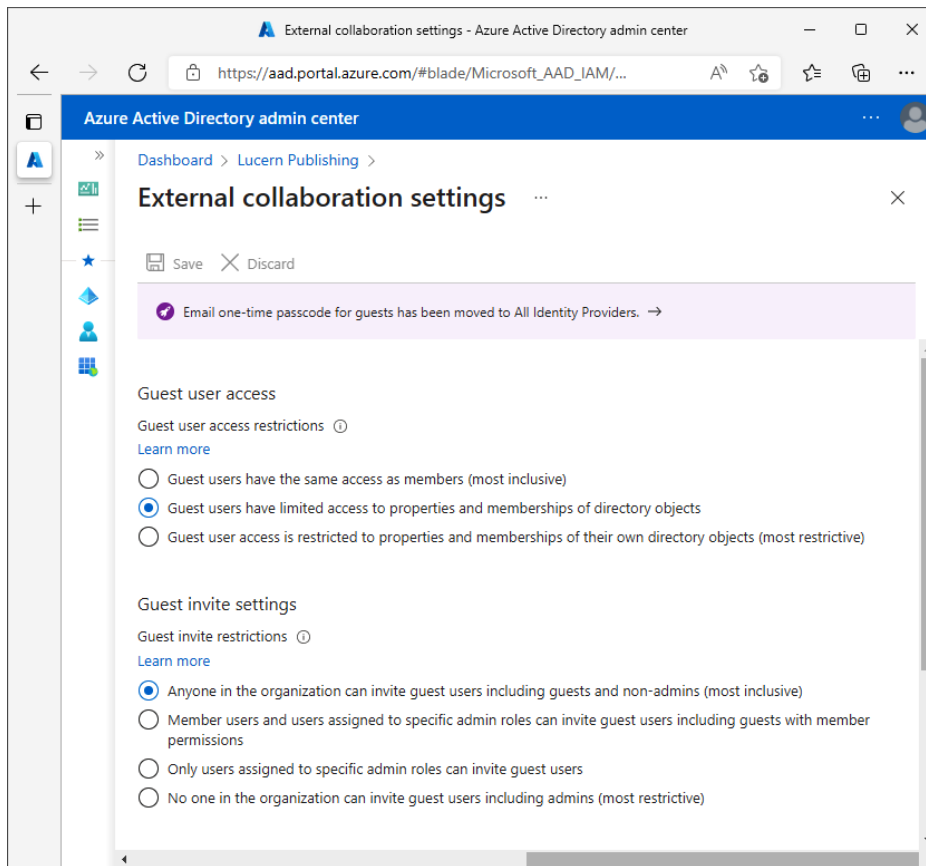
PreviousNext

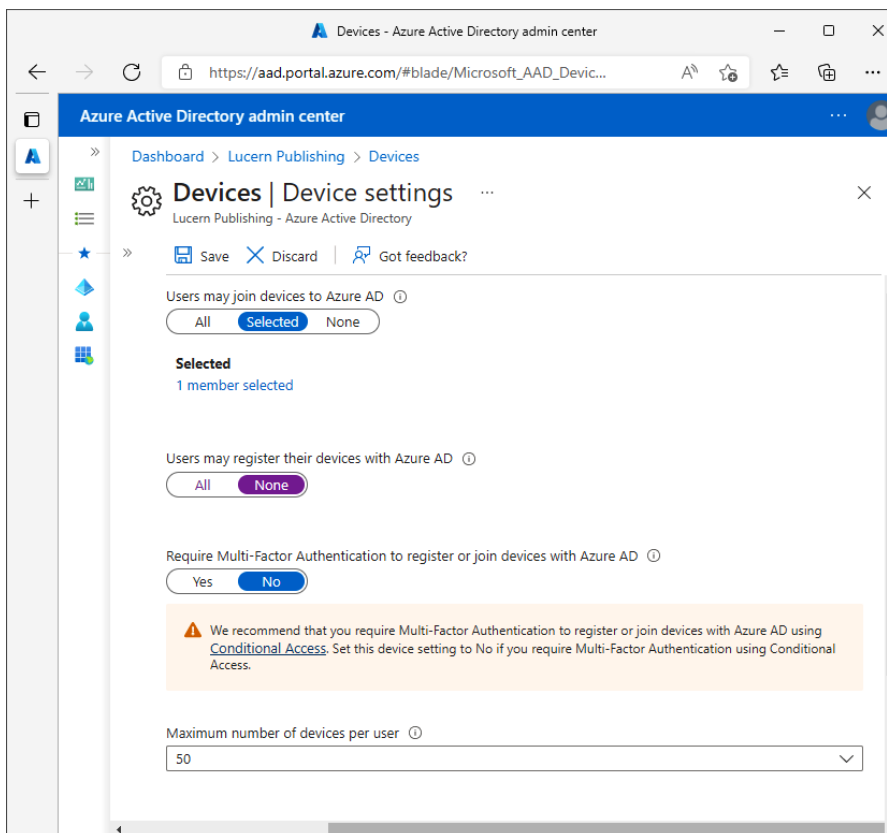
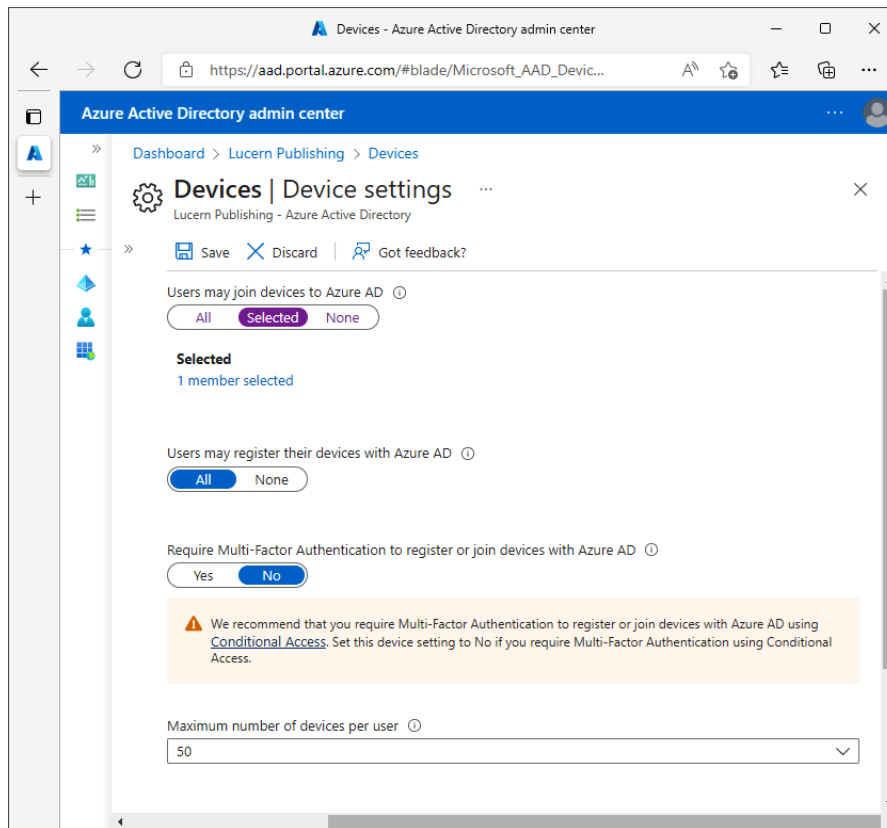


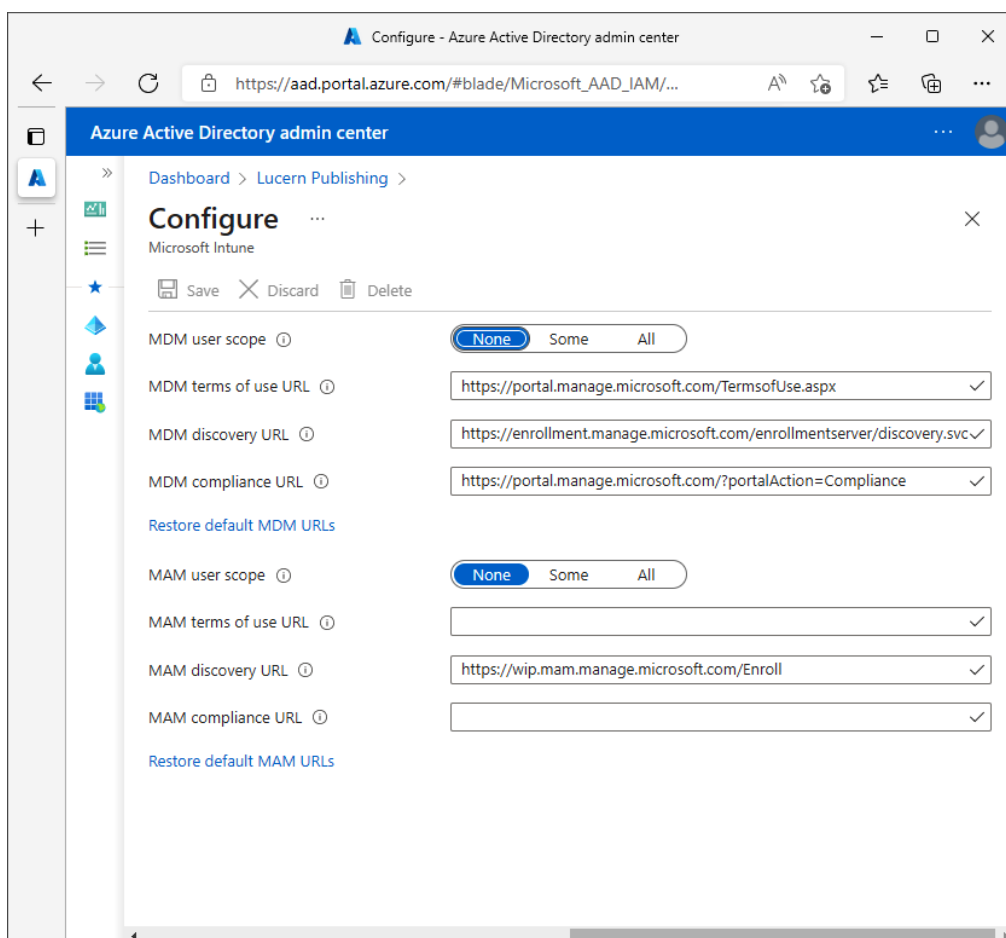
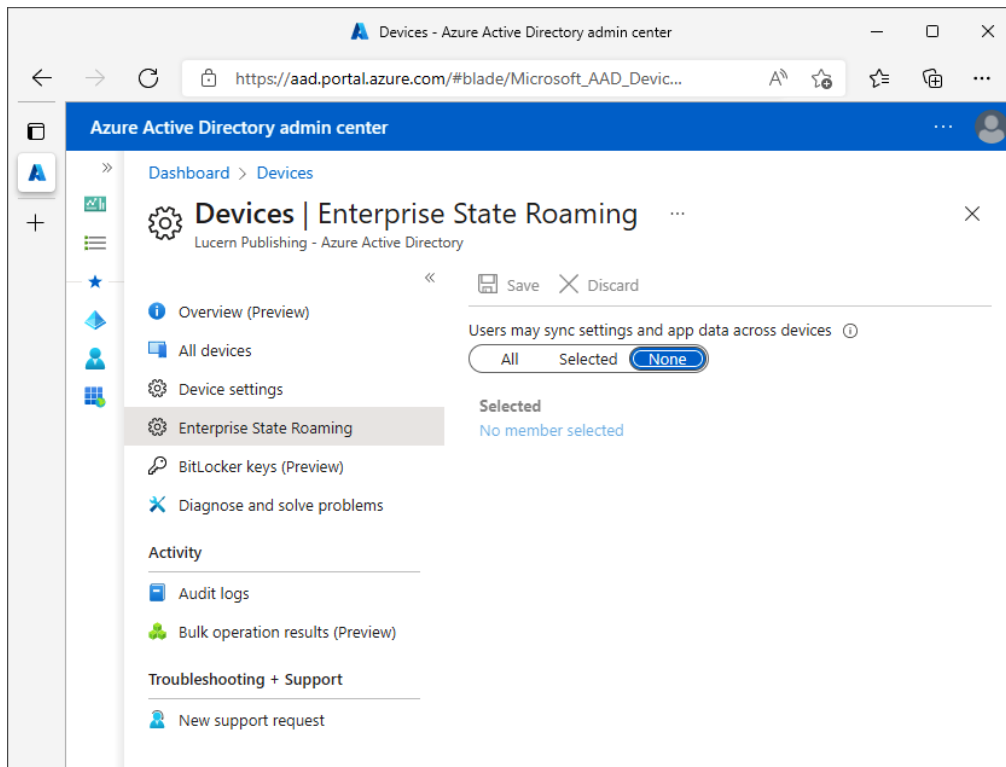
Chapter 16: Hardening Azure AD

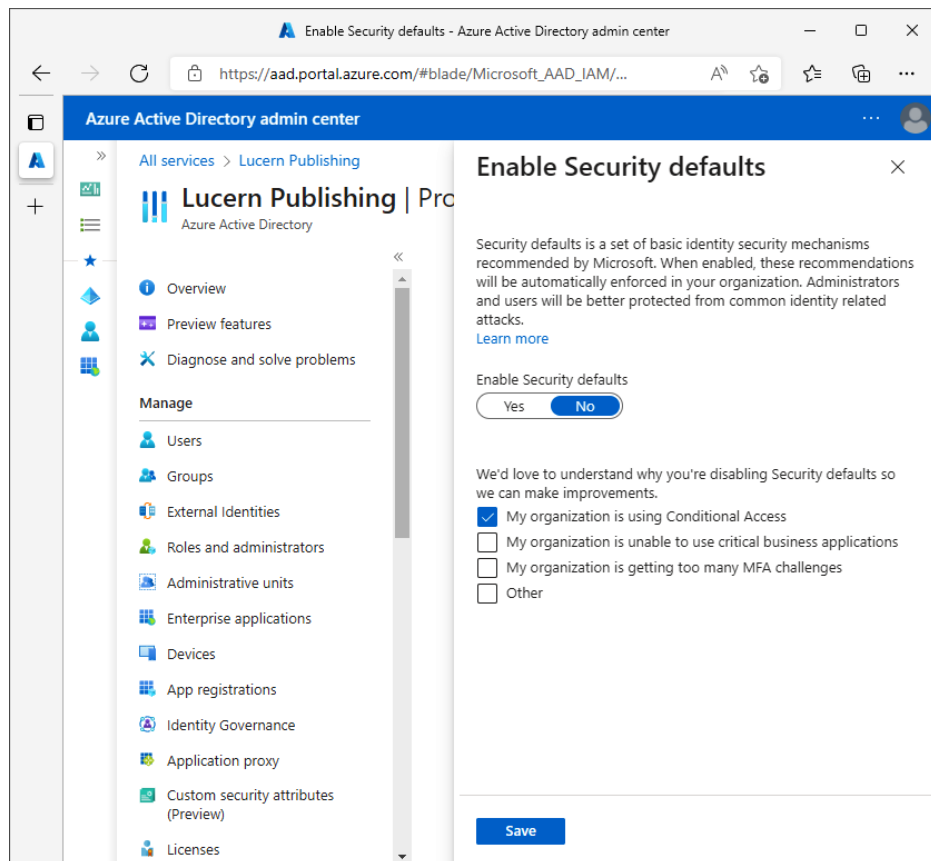
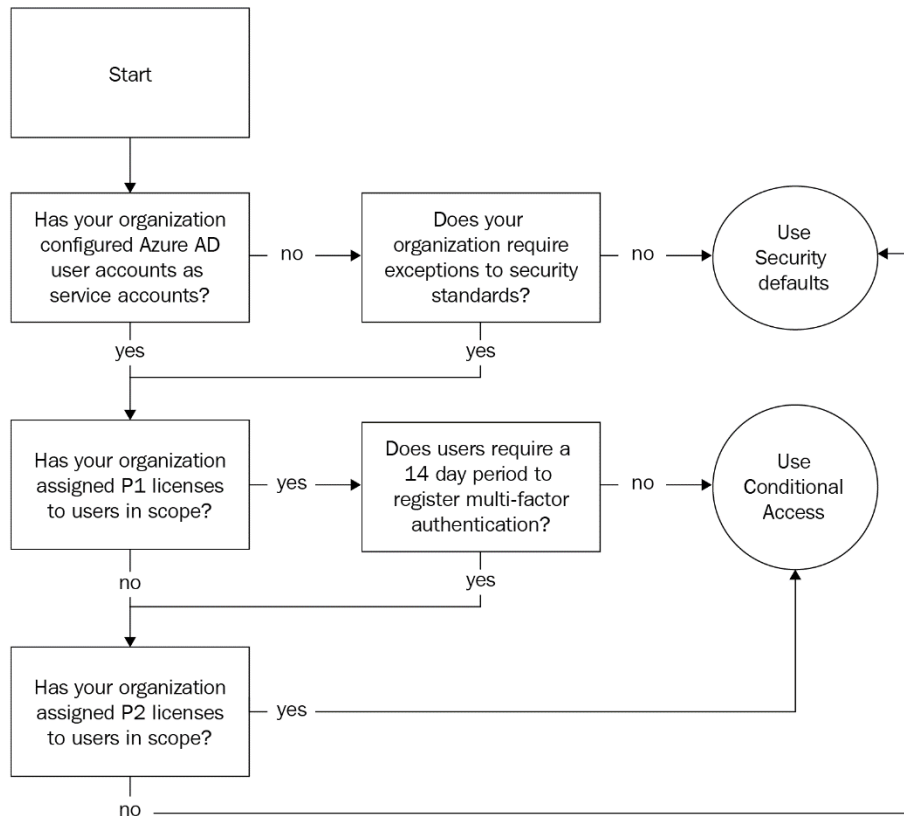


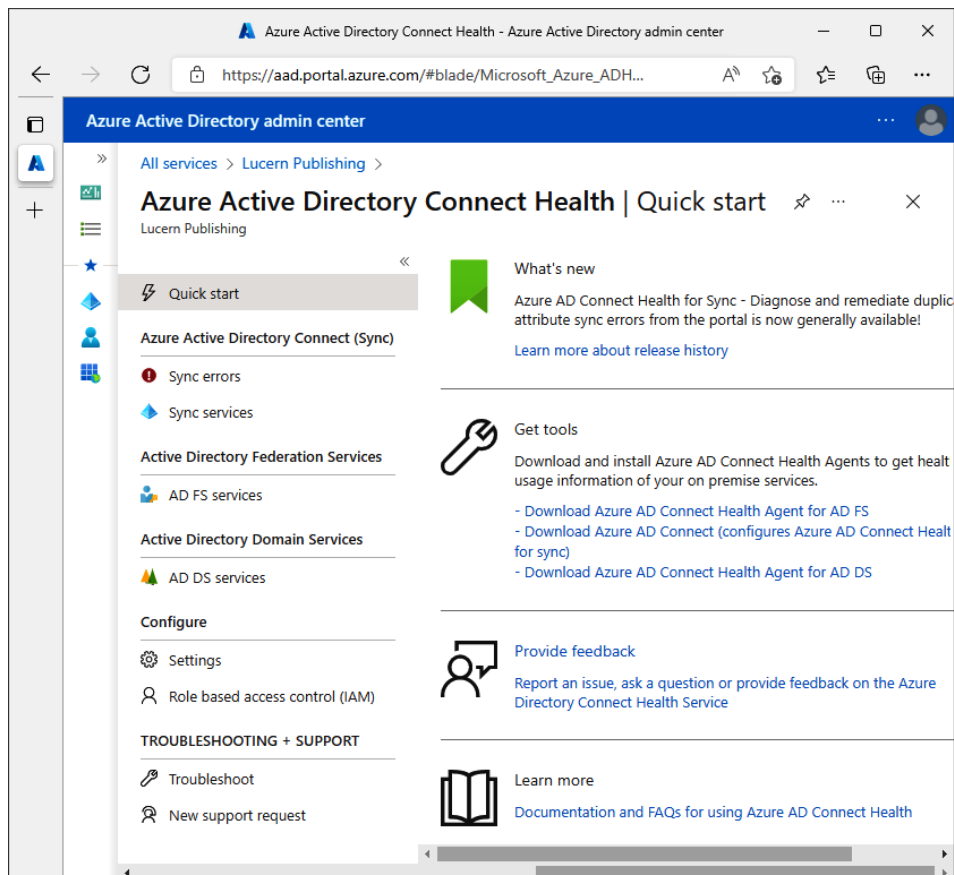
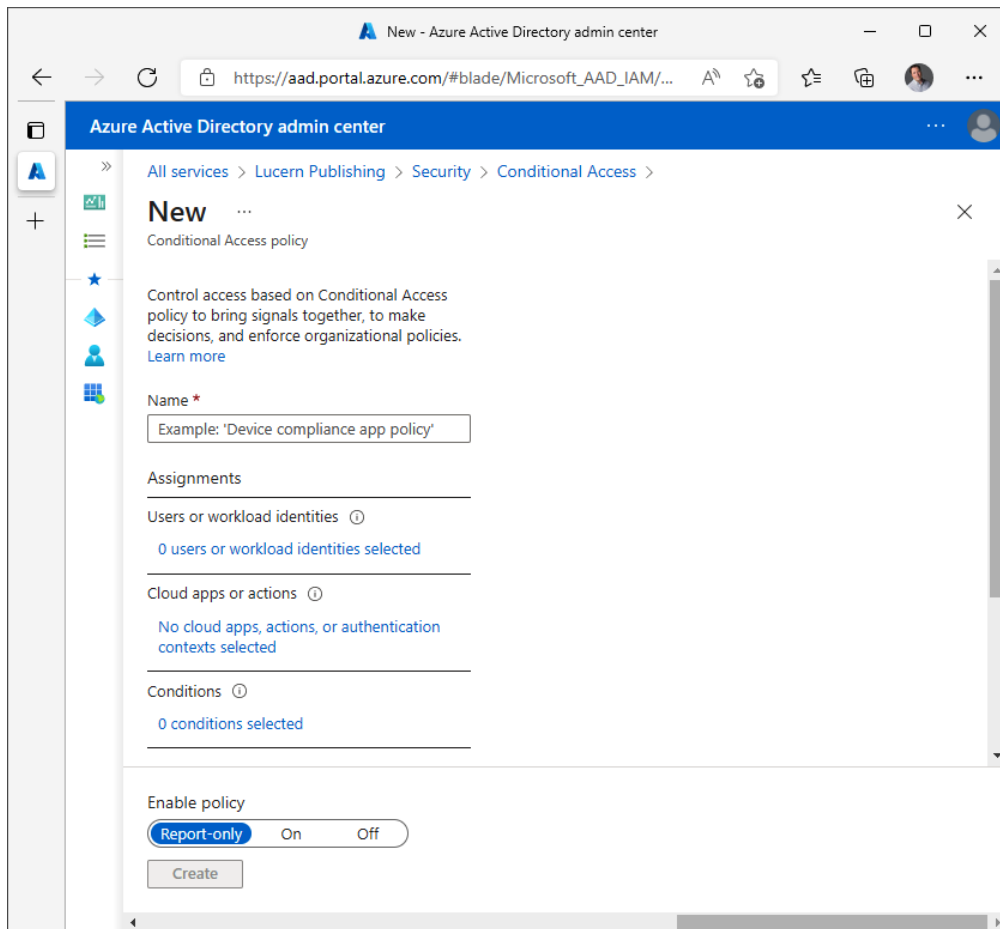


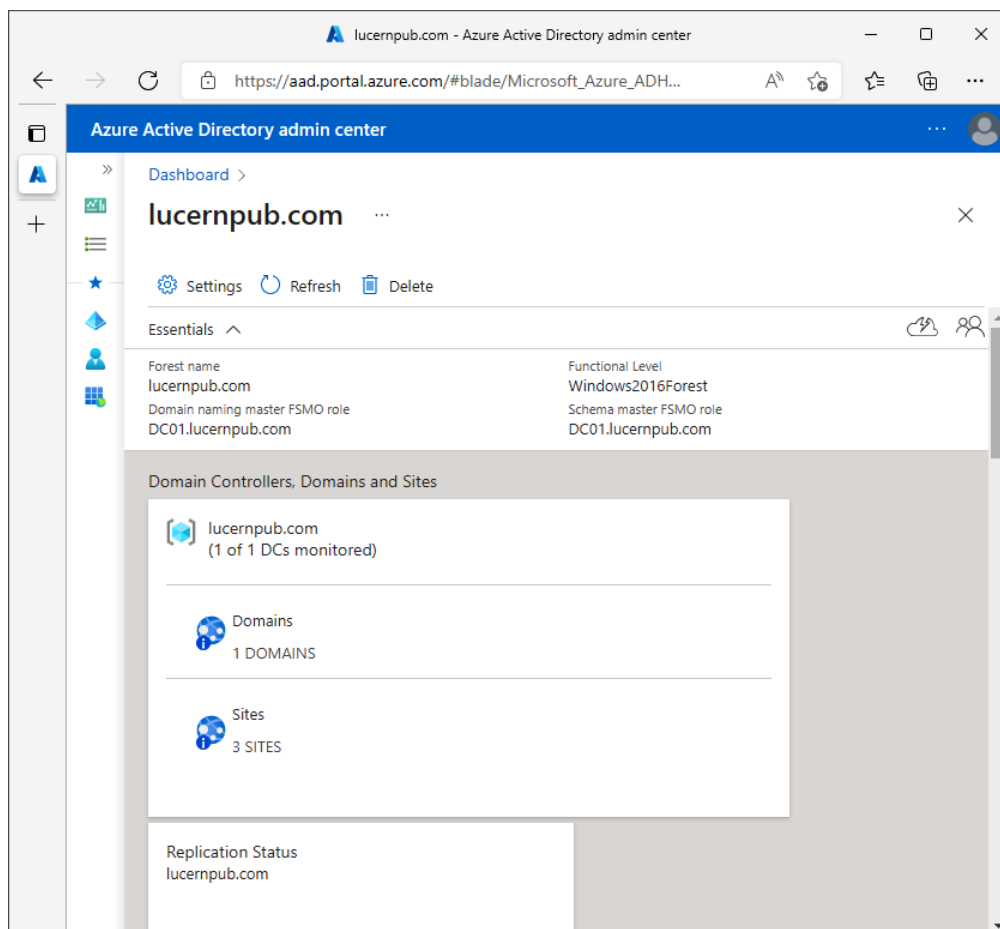
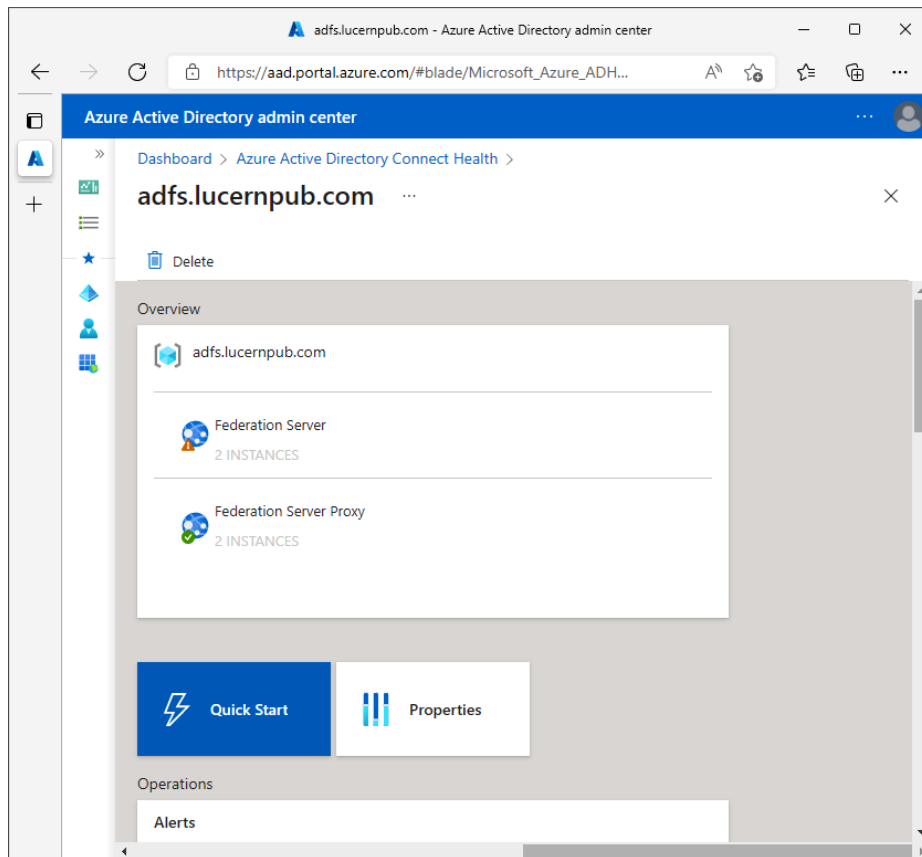












Microsoft Azure

Search resources, services, and docs (G+/)

Home > Privileged Identity Management > Lucern Publishing >

Add assignments

Privileged Identity Management | Azure AD roles

Membership

Setting

Resource

Lucern Publishing

Resource type

Directory

Select role ⓘ

Search role

Select member(s) * ⓘ

No member selected

Next >

Cancel

Microsoft Azure

Search resources, services, and docs (G+/)

Home > Lucern Publishing >

Role setting details - Conditional Access Administrator

Privileged Identity Management | Azure AD roles

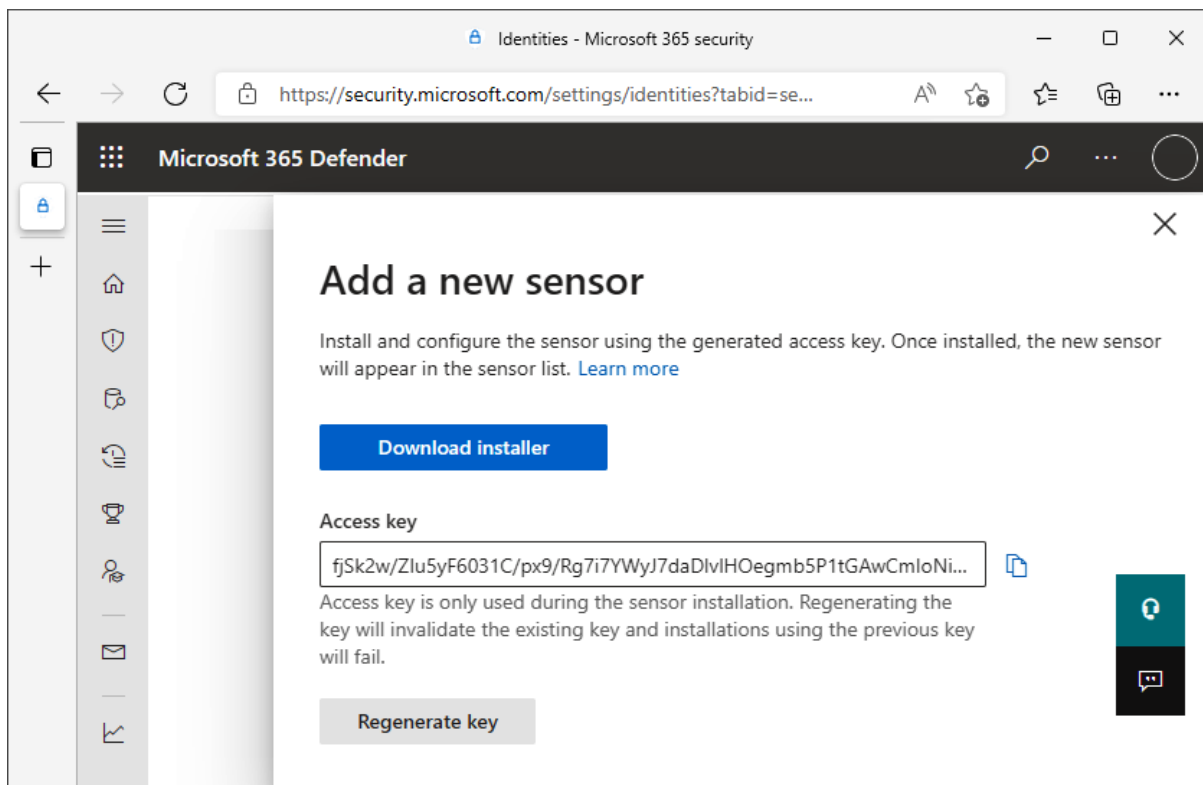
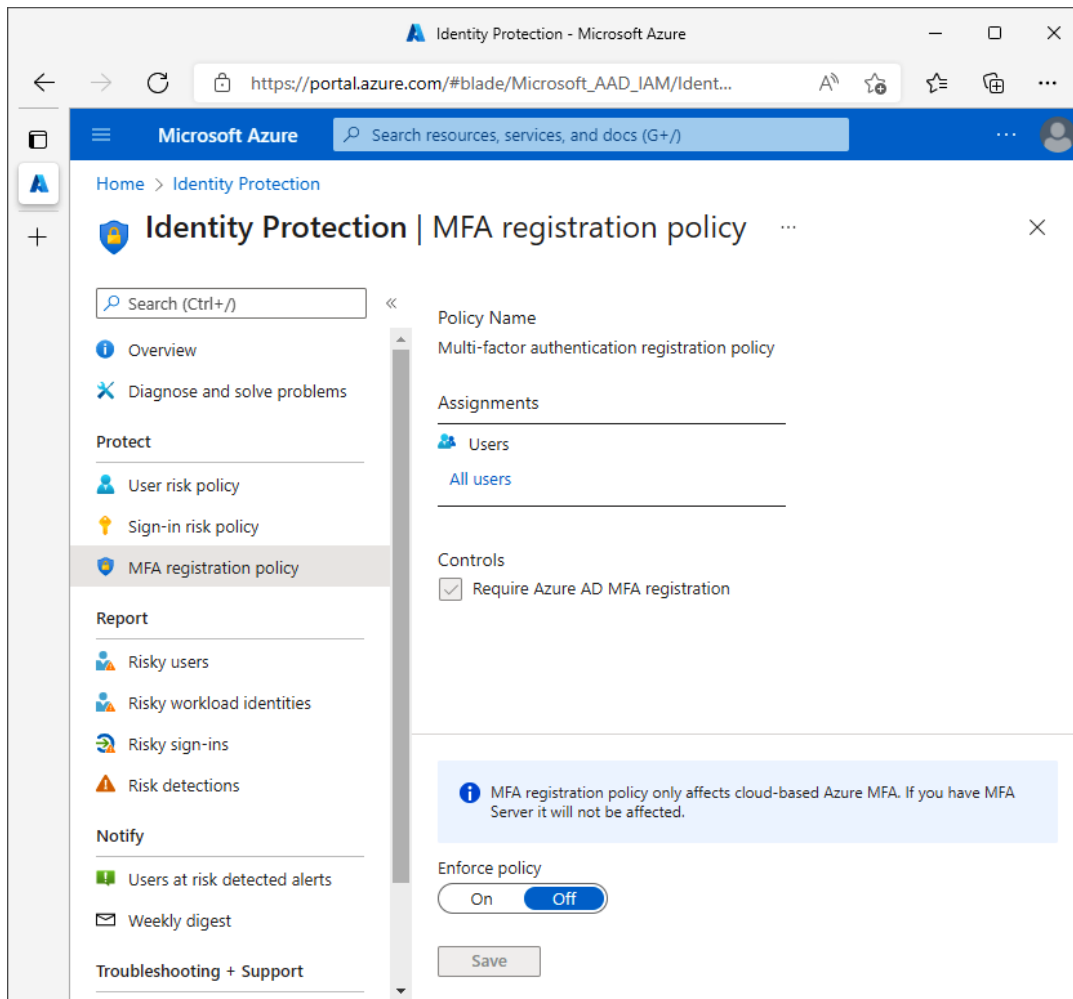
Edit

Activation

Setting	State
Activation maximum duration (hours)	8 hour(s)
Require justification on activation	Yes
Require ticket information on activation	No
On activation, require Azure MFA	Yes
Require approval to activate	No
Approvers	None

Assignment

Setting	State
Allow permanent eligible assignment	Yes
Expire eligible assignments after	-
Allow permanent active assignment	Yes
Expire active assignments after	-



Microsoft
Defender for
Identity



Installation completed successfully

Finish