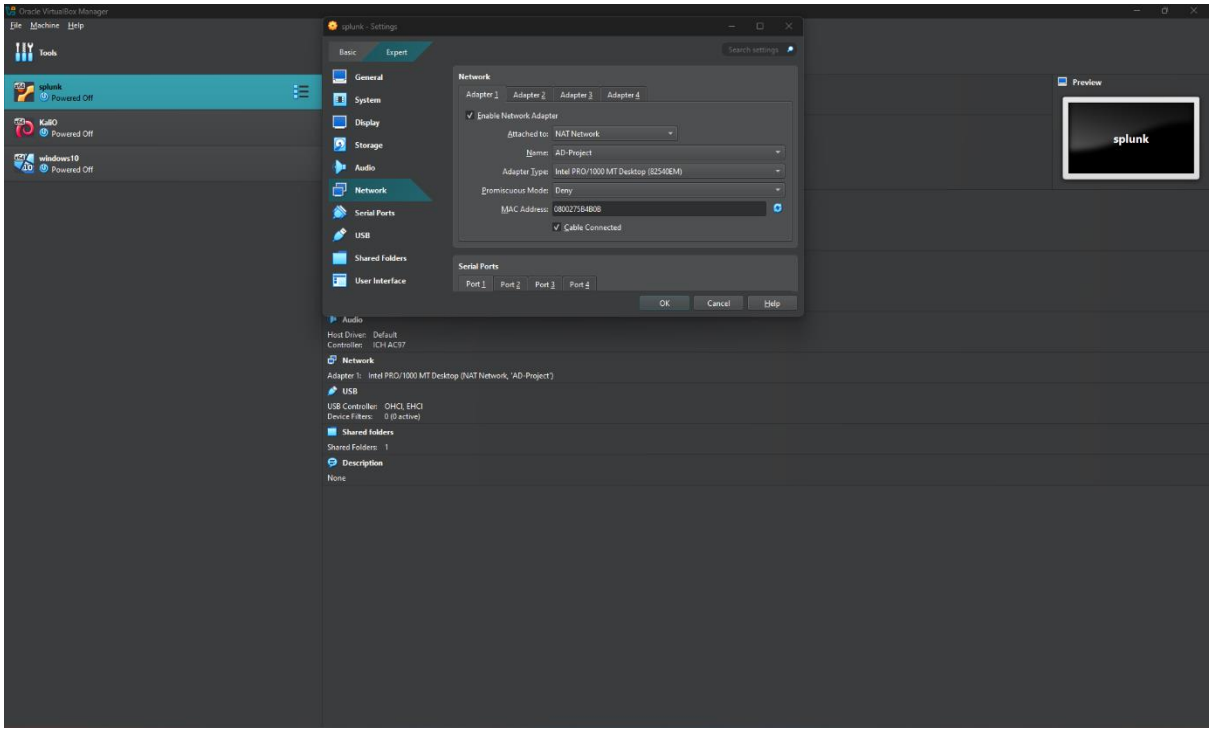



```
Ubuntu 24.04.2 LTS splunk tty1

splunk login: decjag
Password:
Welcome to Ubuntu 24.04.2 LTS (GNU/Linux 6.11.0-19-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

 System information as of Fri Apr 25 03:59:26 PM UTC 2025

  System load:  0.26               Processes:               105
  Usage of /:   79.3% of 11.21GB   Users logged in:         0
  Memory usage: 14%                IPv4 address for enp0s3: 192.168.10.10
  Swap usage:   0%                 IPv4 address for enp0s3: 192.168.10.4


Expanded Security Maintenance for Applications is not enabled.

28 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


The list of available updates is more than a week old.
To check for new updates run: sudo apt update

decjag@splunk:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:5b:4b:0b brd ff:ff:ff:ff:ff:ff
    inet 192.168.10.10/24 brd 192.168.10.255 scope global enp0s3
       valid_lft forever preferred_lft forever
    inet 192.168.10.4/24 metric 100 brd 192.168.10.255 scope global secondary dynamic enp0s3
       valid_lft 467sec preferred_lft 467sec
    inet6 fe80::a00:27ff:fe5b:4b0b/64 scope link
       valid_lft forever preferred_lft forever
decjag@splunk:~$ _
```

```
  GNU nano 7.2                                  /etc/netplan/00-installer-config.yaml
network:
  ethernets:
    enp0s3:
      dhcp4: no
      addresses: [192.168.10.10/24]
      nameservers:
          addresses: [8.8.8.8]
      routes:
          - to: default
            via: 192.168.10.1
  version: 2
```

```
                                [ Read 11 lines ]
^G Help          ^O Write Out    ^W Where Is     ^K Cut          ^T Execute      ^C Location     M-U Undo        M-A Set Mark    M-] To Bracket  M-Q Previous
^X Exit          ^R Read File    ^\ Replace      ^U Paste        ^J Justify      ^/ Go To Line   M-E Redo        M-6 Copy        ^O Where Was    M-W Next
```

```
decjag@splunk:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:5b:4b:0b brd ff:ff:ff:ff:ff:ff
    inet 192.168.10.10/24 brd 192.168.10.255 scope global enp0s3
       valid_lft forever preferred_lft forever
    inet 192.168.10.4/24 metric 100 brd 192.168.10.255 scope global secondary dynamic enp0s3
       valid_lft 583sec preferred_lft 583sec
    inet6 fe80::a00:27ff:fe5b:4b0b/64 scope link
       valid_lft forever preferred_lft forever
decjag@splunk:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=113 time=15.2 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=113 time=14.7 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=113 time=21.8 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=113 time=36.1 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=113 time=20.4 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=113 time=14.4 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=113 time=29.2 ms
64 bytes from 8.8.8.8: icmp_seq=8 ttl=113 time=14.5 ms
64 bytes from 8.8.8.8: icmp_seq=9 ttl=113 time=14.9 ms
64 bytes from 8.8.8.8: icmp_seq=10 ttl=113 time=28.3 ms
64 bytes from 8.8.8.8: icmp_seq=11 ttl=113 time=16.3 ms
64 bytes from 8.8.8.8: icmp_seq=12 ttl=113 time=22.3 ms
64 bytes from 8.8.8.8: icmp_seq=13 ttl=113 time=27.0 ms
64 bytes from 8.8.8.8: icmp_seq=14 ttl=113 time=14.4 ms
64 bytes from 8.8.8.8: icmp_seq=15 ttl=113 time=16.1 ms
64 bytes from 8.8.8.8: icmp_seq=16 ttl=113 time=19.3 ms
^C
--- 8.8.8.8 ping statistics ---
16 packets transmitted, 16 received, 0% packet loss, time 15008ms
rtt min/avg/max/mdev = 14.373/20.307/36.088/6.461 ms
decjag@splunk:~$
```

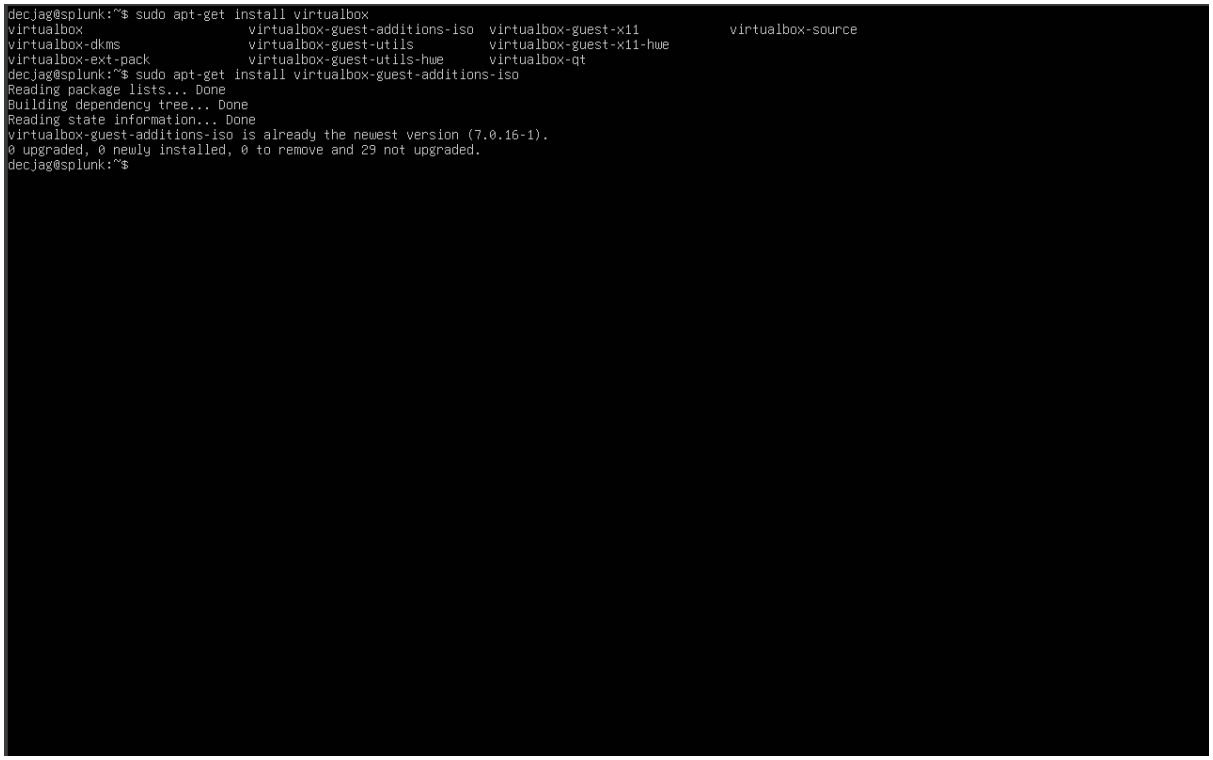
Splunk Enterprise 9.4.1

Index 500 MB/Day. Sign up and download now. After 60 days you can convert to a perpetual free license or purchase a Splunk Enterprise license to continue using the expanded functionality designed for enterprise-scale deployments.

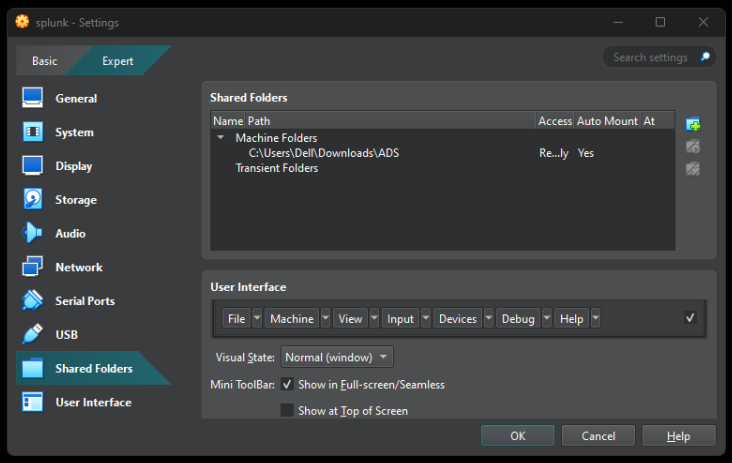
Choose Your Installation Package

Windows | Linux | Mac OS

64-bit	4.x+, 5.x+, 6.x+ kernel Linux distributions	.deb	878.52 MB	Download Now	Copy wget link	More
		.tgz	1177.95 MB	Download Now	Copy wget link	More
		.rpm	1189.2 MB	Download Now	Copy wget link	More



```
decjag@splunk:~$
```




```
decjag@splunk:~$ sudo apt-get install virtualbox
virtualbox                  virtualbox-guest-additions-iso  virtualbox-guest-x11          virtualbox-source
virtualbox-dkms             virtualbox-guest-utils          virtualbox-guest-x11-hwe
virtualbox-ext-pack         virtualbox-guest-utils-hwe      virtualbox-qt
decjag@splunk:~$ sudo apt-get install virtualbox-guest-utlis
[sudo] password for decjag:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
E: Unable to locate package virtualbox-guest-utlis
decjag@splunk:~$ sudo apt-get install virtualbox-guest-utils
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
virtualbox-guest-utils is already the newest version (7.0.16-dfsg-2ubuntu1.1).
0 upgraded, 0 newly installed, 0 to remove and 29 not upgraded.
decjag@splunk:~$ _
```

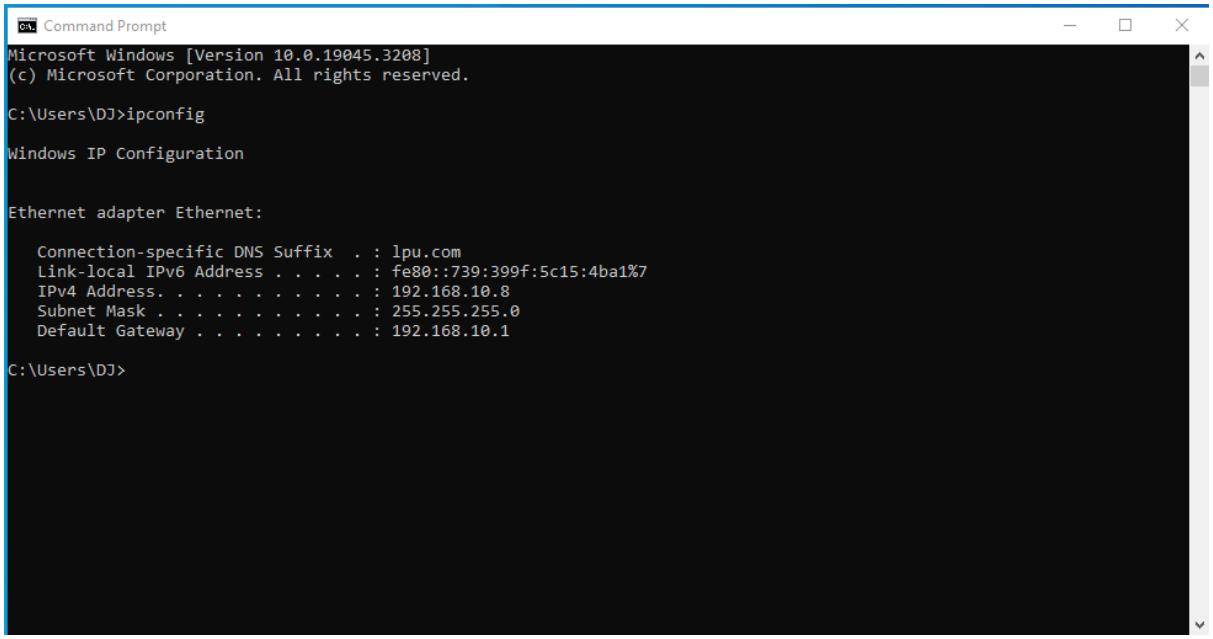
```
decjag@splunk:~$ sudo adduser decjag vboxsf
info: The user `decjag' is already a member of `vboxsf'.
decjag@splunk:~$ mkdir share
decjag@splunk:~$ ls
share  sharedj
decjag@splunk:~$ ls -la
total 40
drwxr-x--- 6 decjag decjag 4096 Apr 25 18:49 .
drwxr-xr-x 3 root   root   4096 Mar 11 06:59 ..
-rw------- 1 decjag decjag  833 Apr 25 18:29 .bash_history
-rw-r--r-- 1 decjag decjag  220 Mar 31  2024 .bash_logout
-rw-r--r-- 1 decjag decjag 3771 Mar 31  2024 .bashrc
drwx------ 2 decjag decjag 4096 Mar 11 07:00 .cache
-rw-r--r-- 1 decjag decjag  807 Mar 31  2024 .profile
drwxrwxr-x 2 decjag decjag 4096 Apr 25 18:49 share
drwxrwxr-x 2 decjag decjag 4096 Mar 11 14:39 sharedj
drwx------ 2 decjag decjag 4096 Mar 11 06:59 .ssh
-rw-r--r-- 1 decjag decjag    0 Mar 11 14:02 .sudo_as_admin_successful
decjag@splunk:~$
```

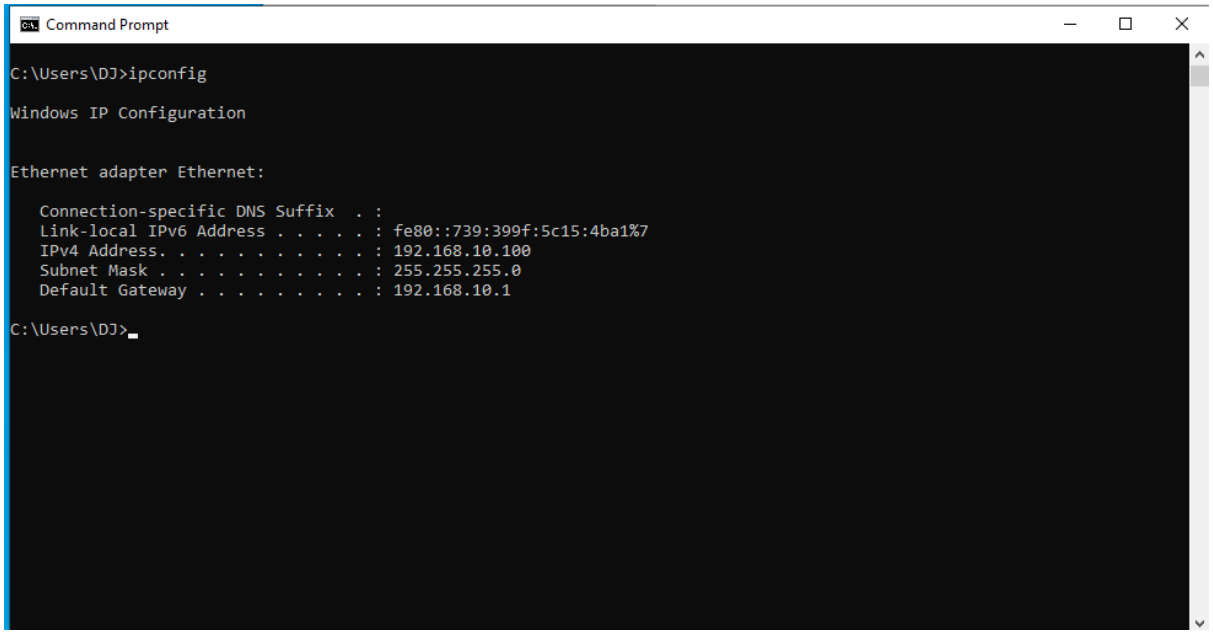
```
decjag@splunk:~$ sudo mount -t vboxsf -o uid=1000,gid=1000 ADS sharedj/
decjag@splunk:~$ ls -la
total 36
drwxr-x--- 6 decjag decjag 4096 Apr 25 18:49 .
drwxr-xr-x 3 root   root   4096 Mar 11 06:59 ..
-rw------- 1 decjag decjag  833 Apr 25 18:29 .bash_history
-rw-r--r-- 1 decjag decjag  220 Mar 31  2024 .bash_logout
-rw-r--r-- 1 decjag decjag 3771 Mar 31  2024 .bashrc
drwx------ 2 decjag decjag 4096 Mar 11 07:00 .cache
-rw-r--r-- 1 decjag decjag  807 Mar 31  2024 .profile
drwxrwxr-x 2 decjag decjag 4096 Apr 25 18:49 share
drwxrwxrwx 1 decjag decjag    0 Mar 10 15:37 sharedj
drwx------ 2 decjag decjag 4096 Mar 11 06:59 .ssh
-rw-r--r-- 1 decjag decjag    0 Mar 11 14:02 .sudo_as_admin_successful
decjag@splunk:~$
```

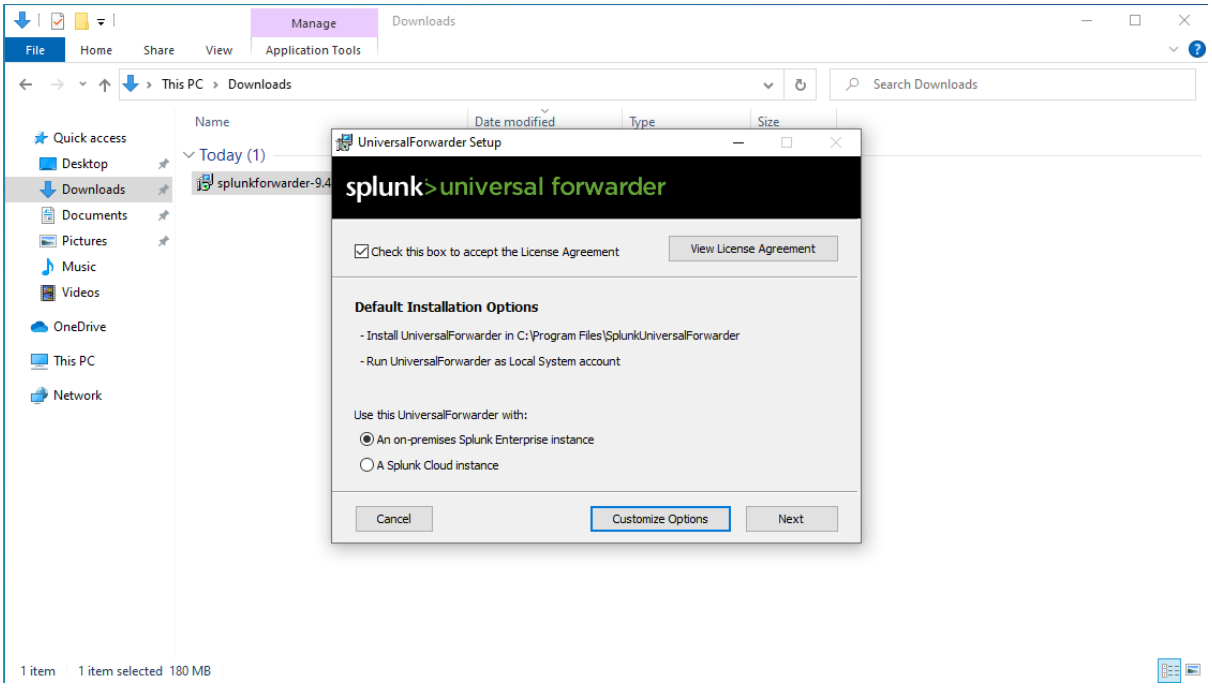
```
decjag@splunk:~$ cd sharedj
decjag@splunk:~/sharedj$ ls -la
total 899612
drwxrwxrwx 1 decjag decjag         0 Mar 10 15:37 .
drwxr-x--- 6 decjag decjag      4096 Apr 25 18:49 ..
-rwxrwxrwx 1 decjag decjag 921195836 Mar 10 15:13 splunk-9.4.1-e3bdab203ac8-linux-amd64.deb
decjag@splunk:~/sharedj$ sudo dpkg -i splunk-9.4.1-e3bdab203ac8-linux-amd64.deb
```

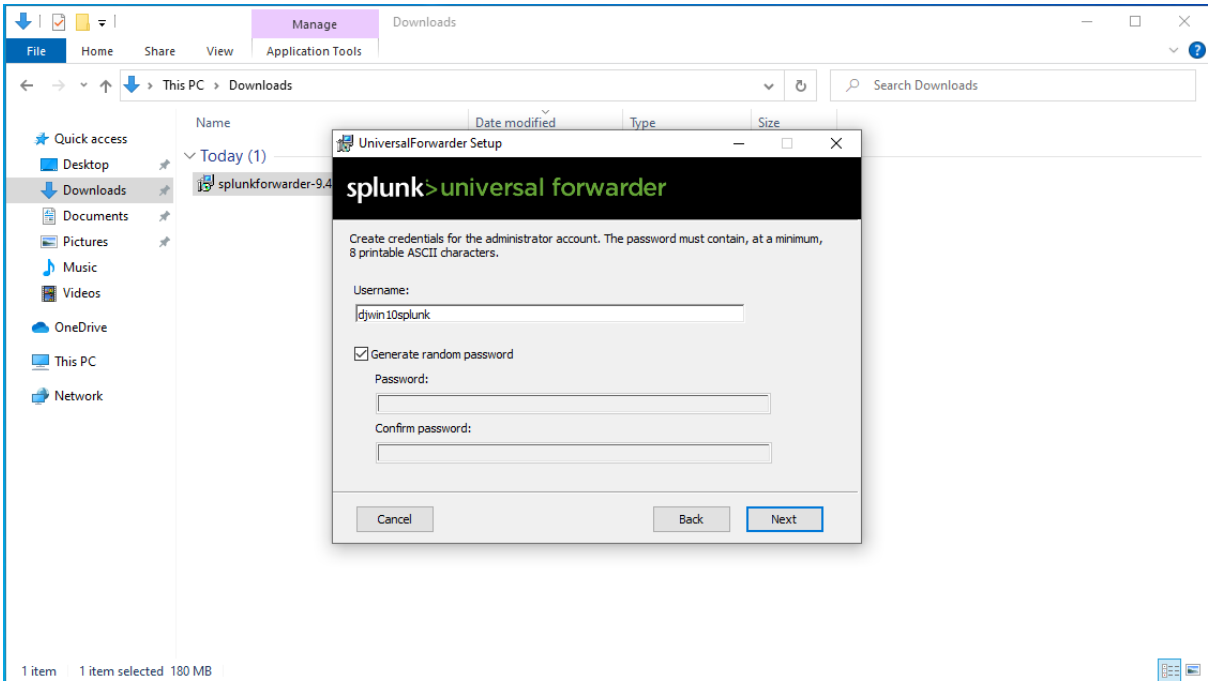
```
decjag@splunk:~$ cd sharedj
decjag@splunk:~/sharedj$ ls -la
total 899612
drwxrwxrwx 1 decjag decjag         0 Mar 10 15:37 .
drwxr-x--- 6 decjag decjag      4096 Apr 25 18:49 ..
-rwxrwxrwx 1 decjag decjag 921195836 Mar 10 15:13 splunk-9.4.1-e3bdab203ac8-linux-amd64.deb
decjag@splunk:~/sharedj$ cd opt/splunk
-bash: cd: opt/splunk: No such file or directory
decjag@splunk:~/sharedj$ cd / opt/splunk
-bash: cd: too many arguments
decjag@splunk:~/sharedj$ cd /opt/splunk
decjag@splunk:/opt/splunk$ ls -la
total 5288
drwxr-xr-x 13 splunk splunk    4096 Apr 25 19:12 .
drwxr-xr-x  3 root   root      4096 Mar 11 15:16 ..
-rw-------  1 splunk splunk     157 Apr 25 19:13 .bash_history
drwxr-xr-x  4 splunk splunk   20480 Apr 25 19:09 bin
-r--r--r--  1 splunk splunk      57 Feb 20 17:58 copyright.txt
drwxr-xr-x 18 splunk splunk    4096 Apr 25 19:12 etc
drwxr-xr-x  4 splunk splunk    4096 Apr 25 19:09 include
drwxr-xr-x 10 splunk splunk   12288 Apr 25 19:09 lib
-r--r--r--  1 splunk splunk   59708 Feb 20 17:58 license-eula.txt
-r--r--r--  1 splunk splunk    1090 Dec 11 20:50 LICENSE.txt
drwxr-xr-x  3 splunk splunk    4096 Mar 11 15:32 openssl
drwxr-xr-x  4 splunk splunk    4096 Mar 11 15:18 opt
drwxr-xr-x  3 splunk splunk    4096 Mar 11 15:33 quarantined_files
-r--r--r--  1 splunk splunk     522 Feb 20 18:03 README-splunk.txt
-rw-------  1 splunk splunk    1024 Mar 11 15:32 .rnd
drwxr-xr-x  5 splunk splunk    4096 Mar 11 15:19 share
drwx--x---  2 splunk splunk    4096 Mar 11 15:32 .splunk
-r--r--r--  1 splunk splunk 5255133 Feb 20 18:30 splunk-9.4.1-e3bdab203ac8-linux-amd64-manifest
drwxr-xr-x  2 splunk splunk    4096 Mar 11 15:19 swidtag
drwx--x---  8 splunk splunk    4096 Mar 11 15:32 var
decjag@splunk:/opt/splunk$ sudo -u splunk bash
[sudo] password for decjag:
splunk@splunk:~$ cd bin
splunk@splunk:~/bin$ ./splunk start
The splunk daemon (splunkd) is already running.


If you get stuck, we're here to help.
Look for answers here: http://docs.splunk.com

The Splunk web interface is at http://splunk:8000

splunk@splunk:~/bin$
```

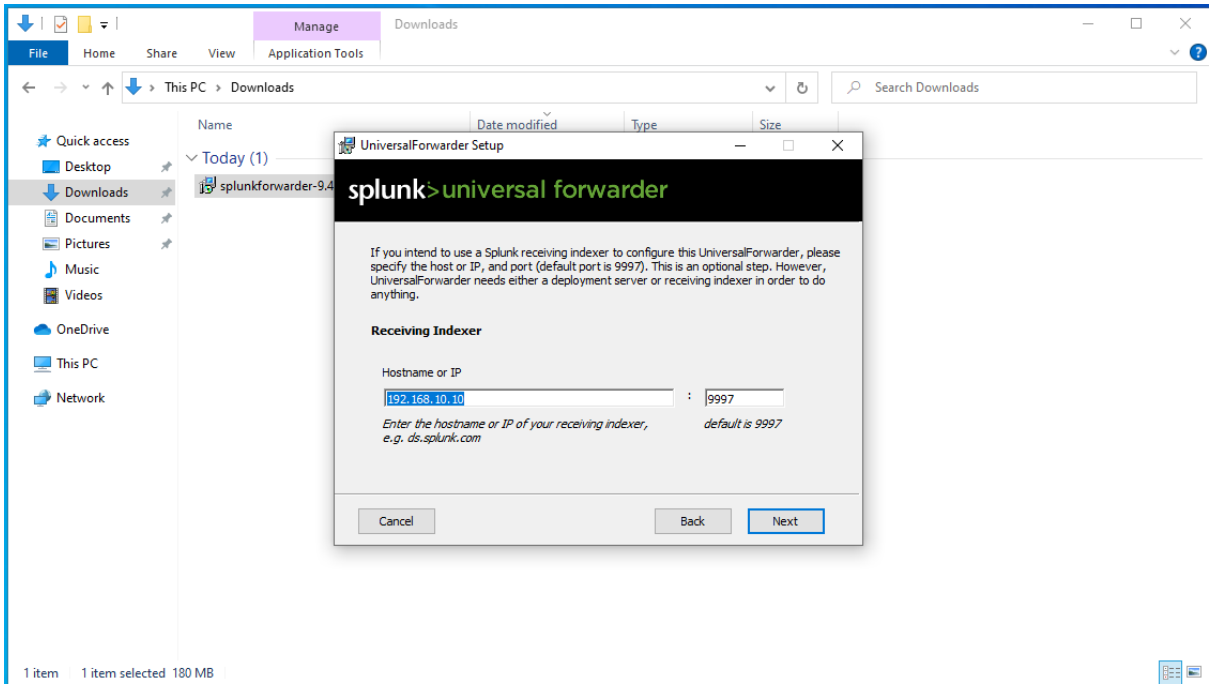
```
splunk@splunk:~/bin$ exit
exit
decjag@splunk:/opt/splunk$ cd bin
decjag@splunk:/opt/splunk/bin$ sudo /splunk enable boot-start -user splunk
sudo: /splunk: command not found
decjag@splunk:/opt/splunk/bin$ sudo ./splunk enable boot-start -user splunk
Init script installed at /etc/init.d/splunk.
Init script is configured to run at boot.
decjag@splunk:/opt/splunk/bin$ _
```

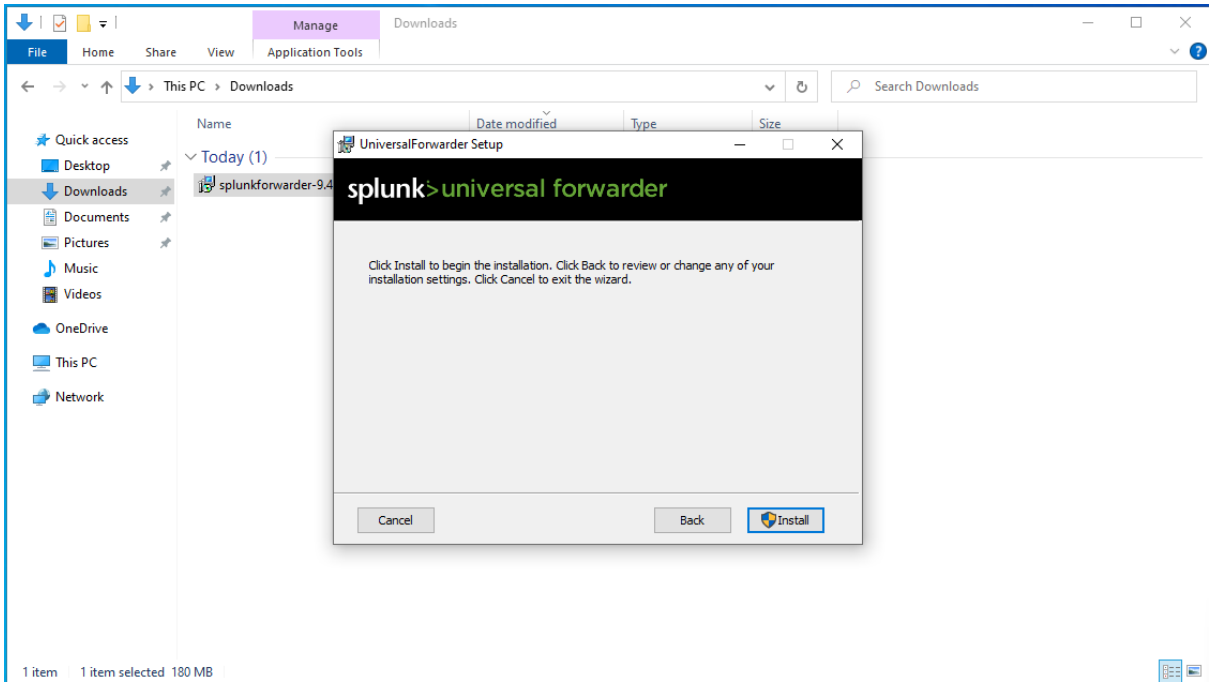

Command Prompt
Microsoft Windows [Version 10.0.19045.3208]
(c) Microsoft Corporation. All rights reserved.
C:\Users\DJ>ipconfig
Windows IP Configuration
Ethernet adapter Ethernet:
Connection-specific DNS Suffix . : lpu.com
Link-local IPv6 Address . . . . . : fe80::739:399f:5c15:4ba1%7
IPv4 Address. . . . . : 192.168.10.8
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.10.1
C:\Users\DJ>

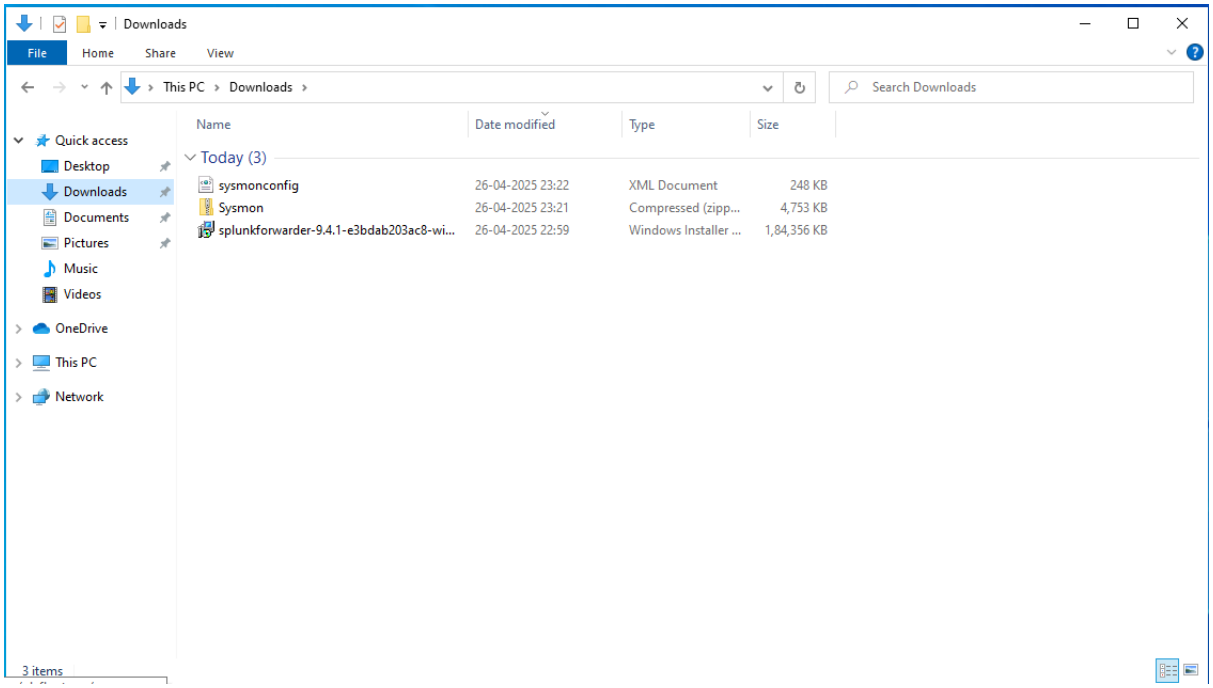

Command Prompt
C:\Users\DJ>ipconfig
Windows IP Configuration
Ethernet adapter Ethernet:
Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::739:399f:5c15:4ba1%7
IPv4 Address. . . . . : 192.168.10.100
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.10.1
C:\Users\DJ>

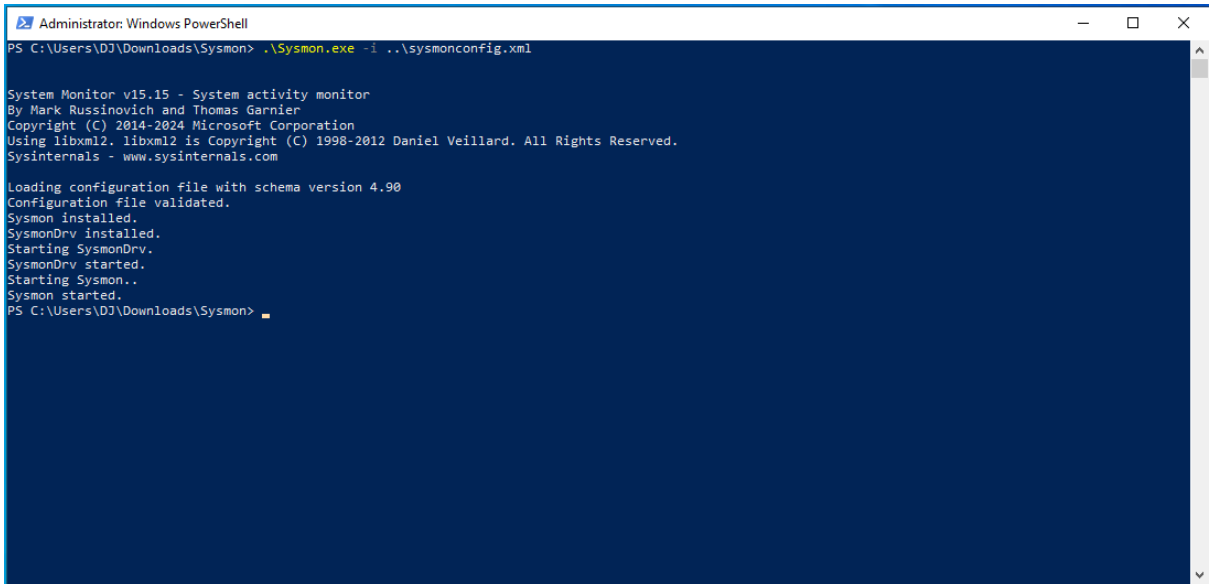

Manage
Downloads
File
Home
Share
View
Application Tools
This PC › Downloads
Search Downloads
Quick access
Desktop
Downloads
Documents
Pictures
Music
Videos
OneDrive
This PC
Network
Name
Date modified
Type
Size
Today (1)
splunkforwarder-9.4
UniversalForwarder Setup
splunk>universal forwarder
Check this box to accept the License Agreement
View License Agreement
Default Installation Options
- Install UniversalForwarder in C:\Program Files\SplunkUniversalForwarder
- Run UniversalForwarder as Local System account
Use this UniversalForwarder with:
An on-premises Splunk Enterprise instance
A Splunk Cloud instance
Cancel
Customize Options
Next
1 item
1 item selected 180 MB

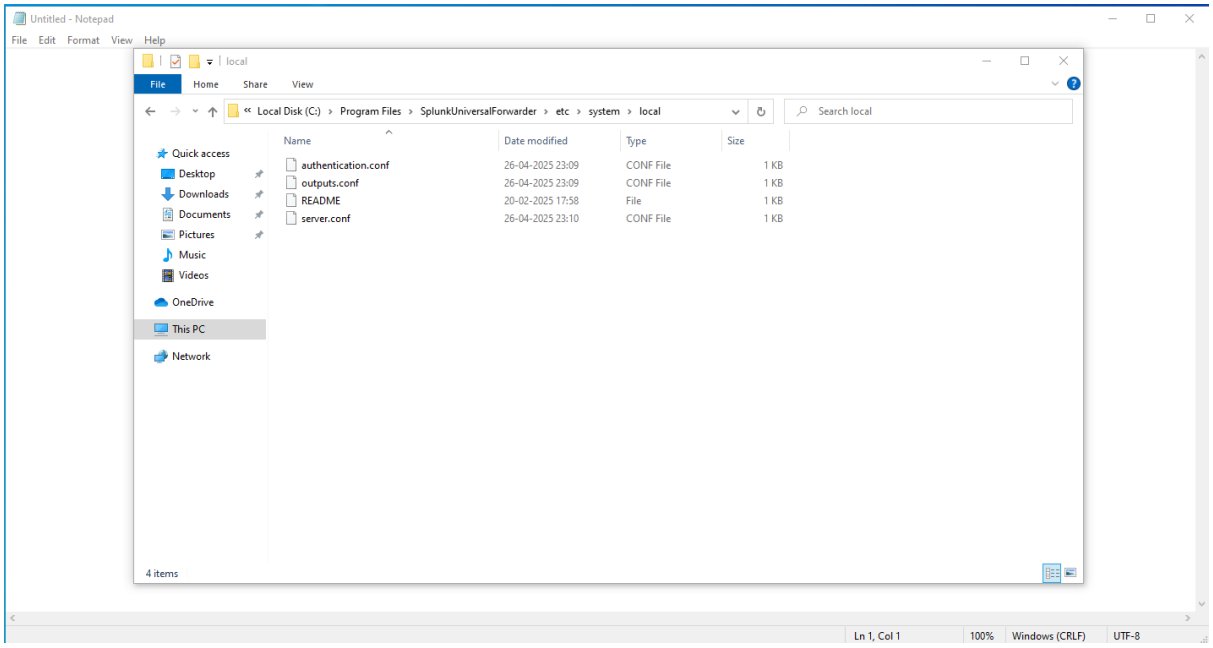

Manage
Downloads
File
Home
Share
View
Application Tools
This PC › Downloads
Search Downloads
Quick access
Desktop
Downloads
Documents
Pictures
Music
Videos
OneDrive
This PC
Network
Name
Date modified
Type
Size
Today (1)
splunkforwarder-9.4
UniversalForwarder Setup
splunk>universal forwarder
Create credentials for the administrator account. The password must contain, at a minimum, 8 printable ASCII characters.
Username:
djwin10splunk
Generate random password
Password:
Confirm password:
Cancel
Back
Next
1 item
1 item selected 180 MB

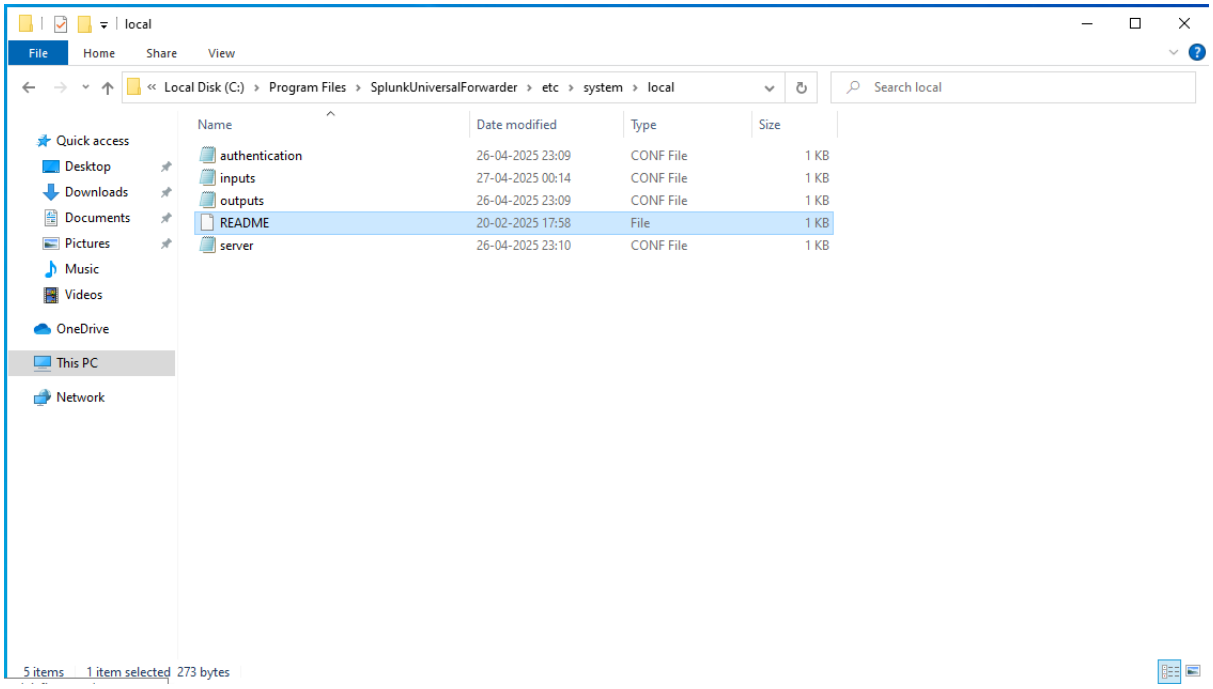

Manage
Downloads
File
Home
Share
View
Application Tools
This PC › Downloads
Search Downloads
Quick access
Desktop
Downloads
Documents
Pictures
Music
Videos
OneDrive
This PC
Network
Name
Date modified
Type
Size
Today (1)
splunkforwarder-9.4
UniversalForwarder Setup
splunk>universal forwarder
If you intend to use a Splunk receiving indexer to configure this UniversalForwarder, please specify the host or IP, and port (default port is 9997). This is an optional step. However, UniversalForwarder needs either a deployment server or receiving indexer in order to do anything.
Receiving Indexer
Hostname or IP
192.168.10.10
9997
Enter the hostname or IP of your receiving indexer, e.g. ds.splunk.com
default is 9997
Cancel
Back
Next
1 item
1 item selected 180 MB

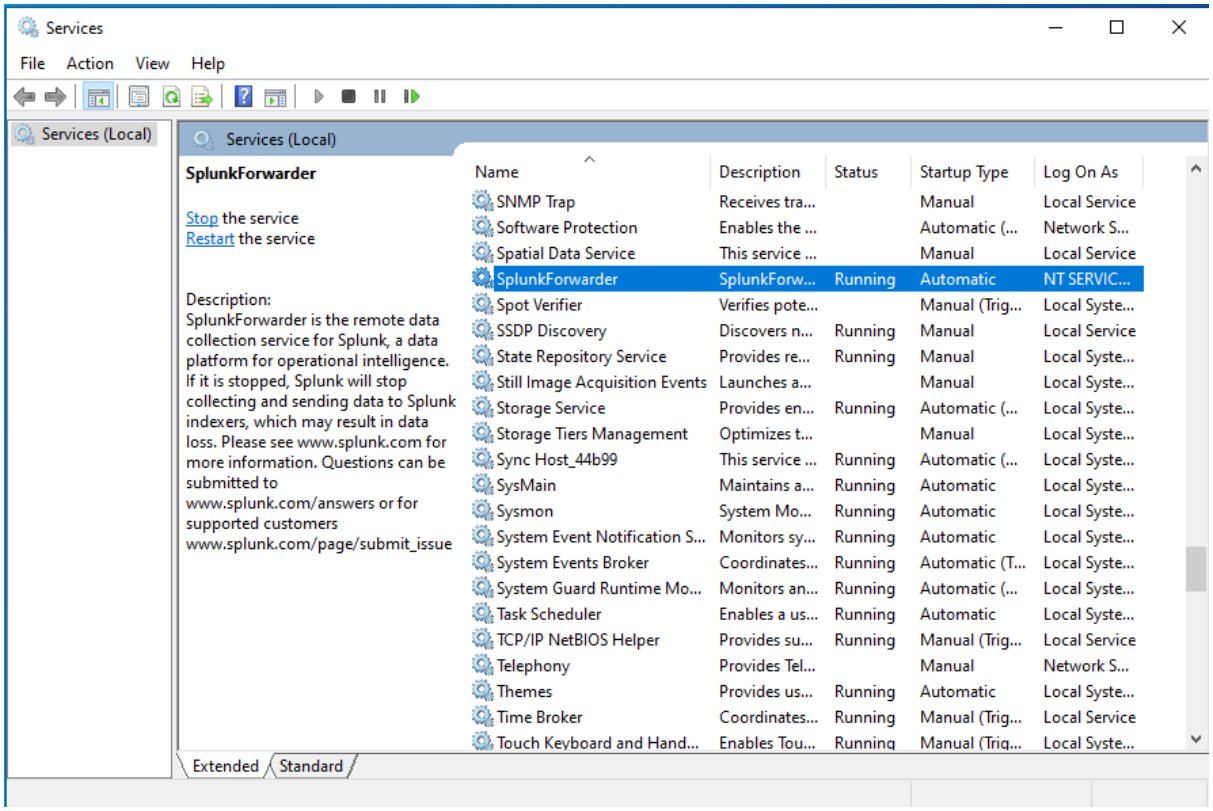

Manage
Downloads
File
Home
Share
View
Application Tools
This PC › Downloads
Search Downloads
Quick access
Desktop
Downloads
Documents
Pictures
Music
Videos
OneDrive
This PC
Network
Name
Date modified
Type
Size
Today (1)
splunkforwarder-9.4
UniversalForwarder Setup
splunk>universal forwarder
Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.
Cancel
Back
Install
1 item
1 item selected 180 MB

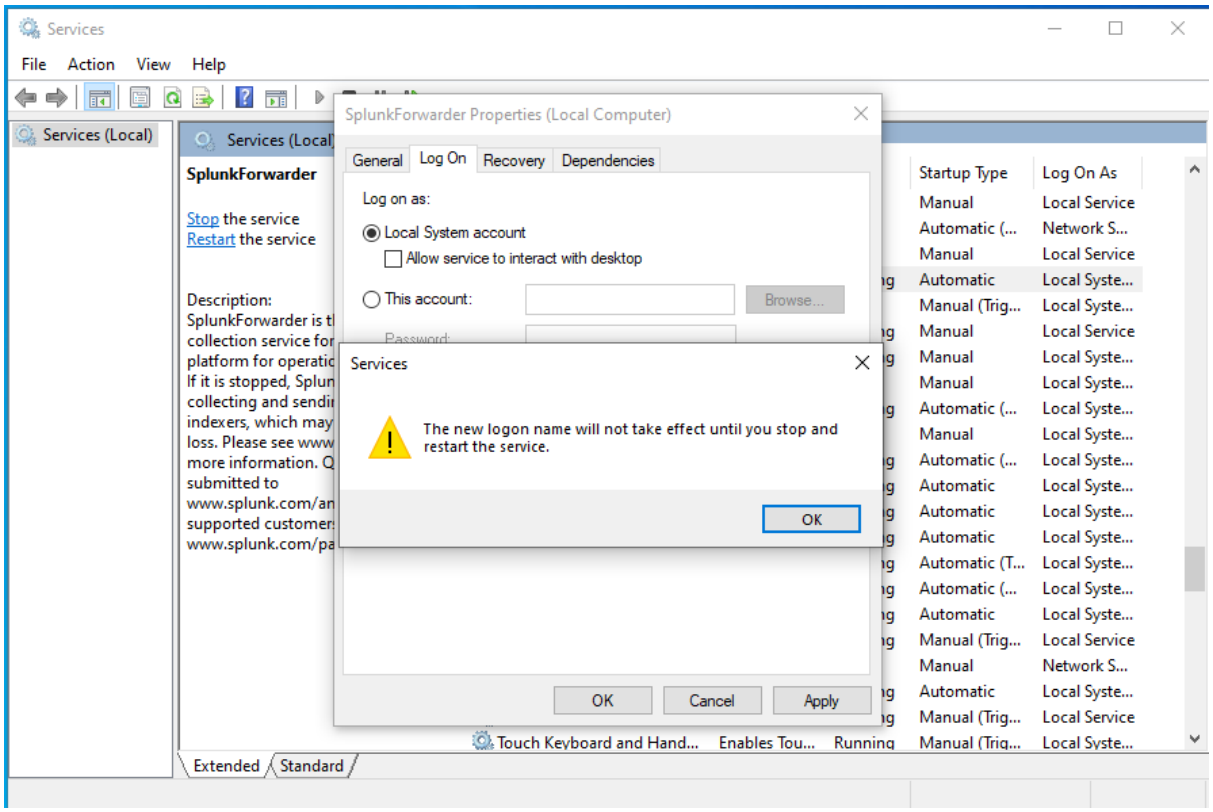

Downloads
File
Home
Share
View
This PC › Downloads ›
Search Downloads
Quick access
Desktop
Downloads
Documents
Pictures
Music
Videos
OneDrive
This PC
Network
Name
Date modified
Type
Size
Today (3)
sysmonconfig
26-04-2025 23:22
XML Document
248 KB
Sysmon
26-04-2025 23:21
Compressed (zipp...
4,753 KB
splunkforwarder-9.4.1-e3bdab203ac8-wi...
26-04-2025 22:59
Windows Installer ...
1,84,356 KB
3 items

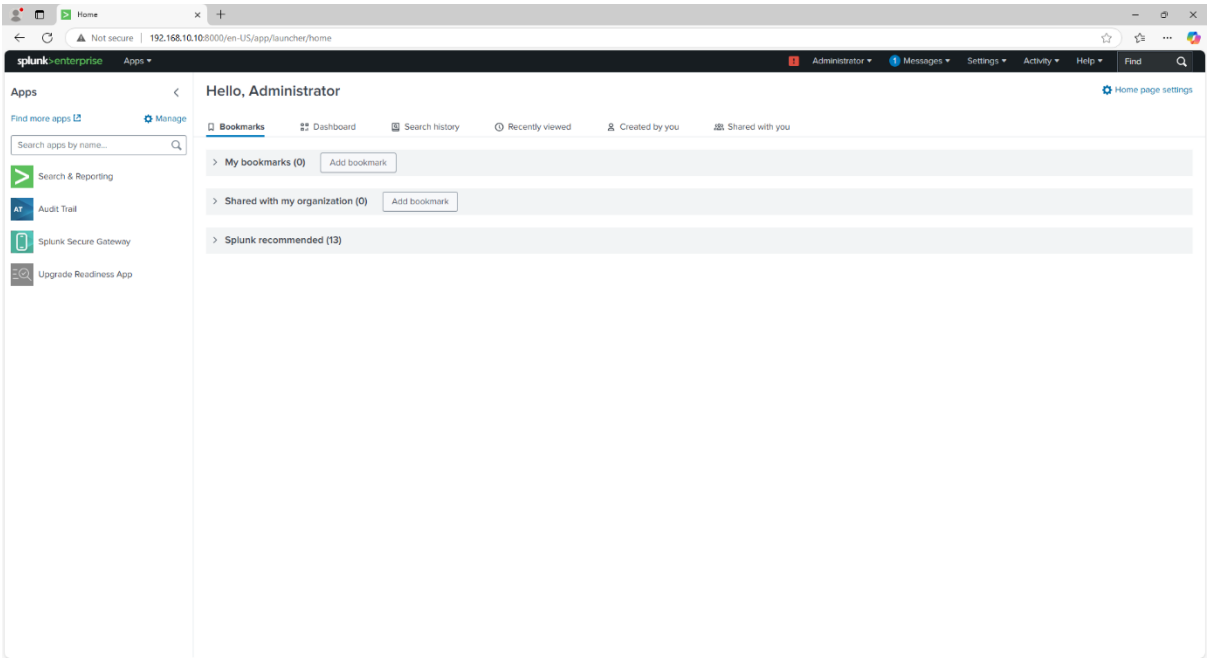

Administrator: Windows PowerShell
PS C:\Users\DJ\Downloads\Sysmon> .\Sysmon.exe -i ..\sysmonconfig.xml
System Monitor v15.15 - System activity monitor
By Mark Russinovich and Thomas Garnier
Copyright (C) 2014-2024 Microsoft Corporation
Using libxml2. libxml2 is Copyright (C) 1998-2012 Daniel Veillard. All Rights Reserved.
Sysinternals - www.sysinternals.com
Loading configuration file with schema version 4.90
Configuration file validated.
Sysmon installed.
SysmonDrv installed.
Starting SysmonDrv.
SysmonDrv started.
Starting Sysmon..
Sysmon started.
PS C:\Users\DJ\Downloads\Sysmon>

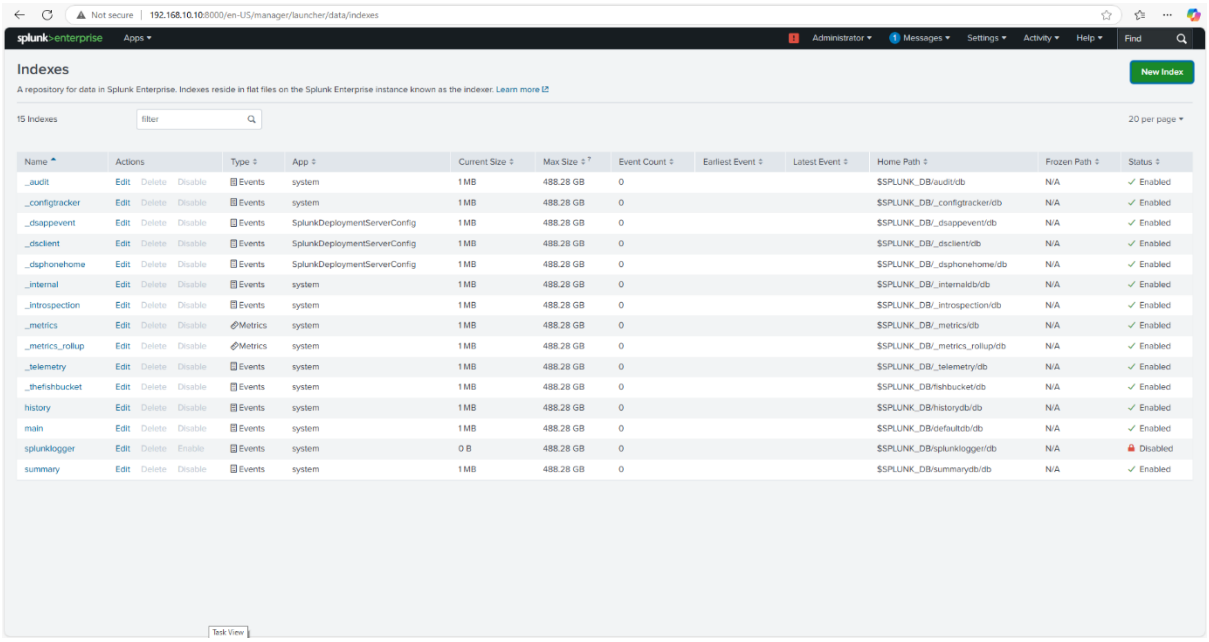

Untitled - Notepad
File Edit Format View Help
local
File Home Share View
Local Disk (C:) › Program Files › SplunkUniversalForwarder › etc › system › local
Search local
Quick access
Desktop
Downloads
Documents
Pictures
Music
Videos
OneDrive
This PC
Network
Name
Date modified
Type
Size
authentication.conf 26-04-2025 23:09 CONF File 1 KB
outputs.conf 26-04-2025 23:09 CONF File 1 KB
README 20-02-2025 17:58 File 1 KB
server.conf 26-04-2025 23:10 CONF File 1 KB
4 items
Ln 1, Col 1
100%
Windows (CRLF)
UTF-8

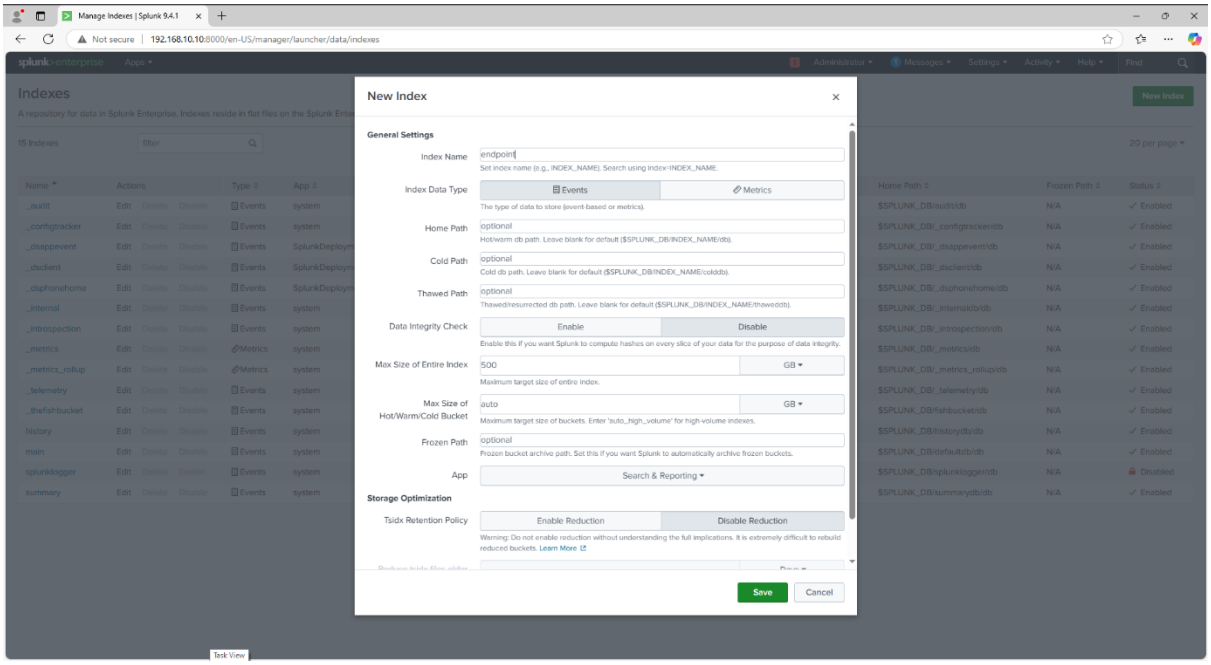

local
File Home Share View
Local Disk (C:) › Program Files › SplunkUniversalForwarder › etc › system › local
Search local
Quick access
Desktop
Downloads
Documents
Pictures
Music
Videos
OneDrive
This PC
Network
Name
Date modified
Type
Size
authentication 26-04-2025 23:09 CONF File 1 KB
inputs 27-04-2025 00:14 CONF File 1 KB
outputs 26-04-2025 23:09 CONF File 1 KB
README 20-02-2025 17:58 File 1 KB
server 26-04-2025 23:10 CONF File 1 KB
5 items 1 item selected 273 bytes

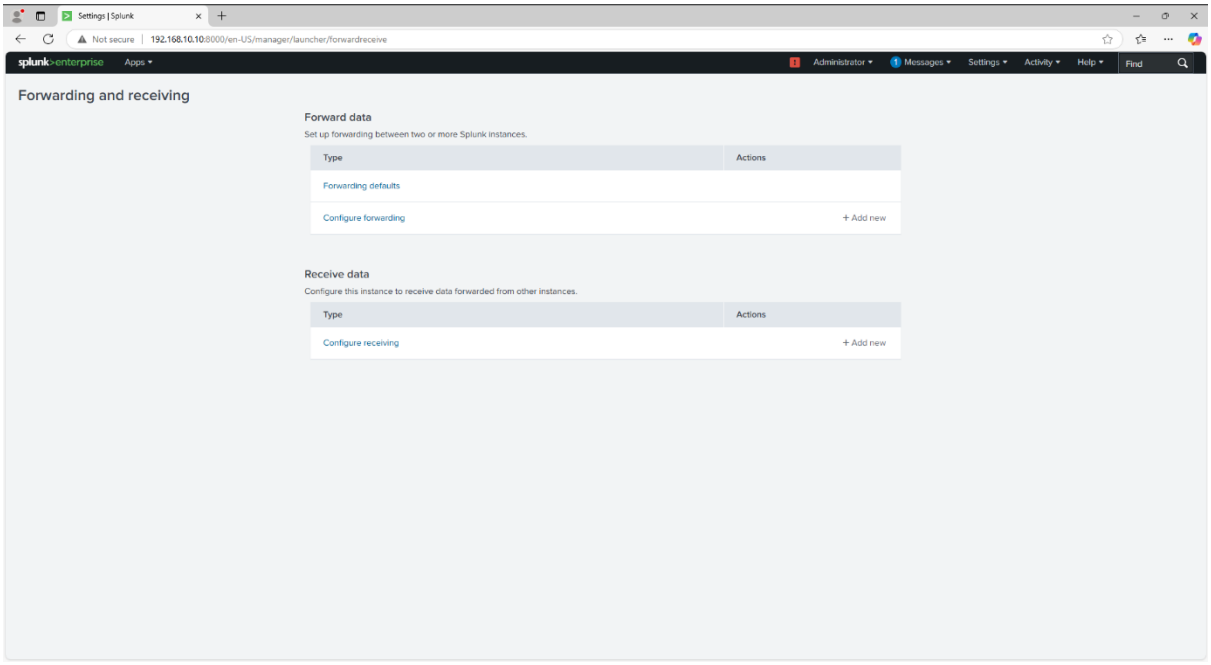

Services
File Action View Help
Services (Local)
Services (Local)
SplunkForwarder
Stop the service
Restart the service
Description:
SplunkForwarder is the remote data collection service for Splunk, a data platform for operational intelligence. If it is stopped, Splunk will stop collecting and sending data to Splunk indexers, which may result in data loss. Please see www.splunk.com for more information. Questions can be submitted to www.splunk.com/answers or for supported customers www.splunk.com/page/submit_issue
Name
Description
Status
Startup Type
Log On As
SNMP Trap Receives tra... Manual Local Service
Software Protection Enables the ... Automatic (... Network S...
Spatial Data Service This service ... Manual Local Service
SplunkForwarder SplunkForw... Running Automatic NT SERVIC...
Spot Verifier Verifies pote... Manual (Trig... Local Syste...
SSDP Discovery Discovers n... Running Manual Local Service
State Repository Service Provides re... Running Manual Local Syste...
Still Image Acquisition Events Launches a... Manual Local Syste...
Storage Service Provides en... Running Automatic (... Local Syste...
Storage Tiers Management Optimizes t... Manual Local Syste...
Sync Host_44b99 This service ... Running Automatic (... Local Syste...
SysMain Maintains a... Running Automatic Local Syste...
Sysmon System Mo... Running Automatic Local Syste...
System Event Notification S... Monitors sy... Running Automatic Local Syste...
System Events Broker Coordinates... Running Automatic (T... Local Syste...
System Guard Runtime Mo... Monitors an... Running Automatic (... Local Syste...
Task Scheduler Enables a us... Running Automatic Local Syste...
TCP/IP NetBIOS Helper Provides su... Running Manual (Trig... Local Service
Telephony Provides Tel... Manual Network S...
Themes Provides us... Running Automatic Local Syste...
Time Broker Coordinates... Running Manual (Trig... Local Service
Touch Keyboard and Hand... Enables Tou... Running Manual (Trig... Local Syste...
Extended
Standard

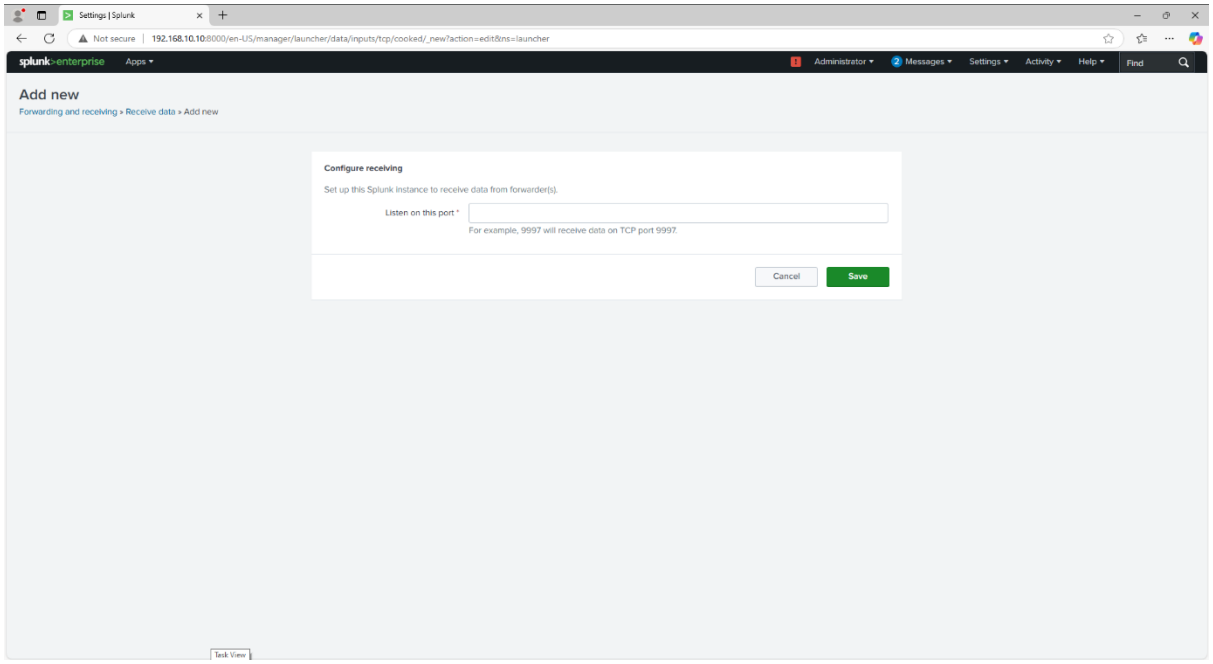

Services
File Action View Help
Services (Local)
SplunkForwarder
Stop the service
Restart the service
SplunkForwarder Properties (Local Computer)
General
Log On
Recovery
Dependencies
Log on as:
Local System account
Allow service to interact with desktop
This account:
Browse...
Password:
Services
The new logon name will not take effect until you stop and restart the service.
OK
OK
Cancel
Apply
Startup Type
Log On As
Touch Keyboard and Hand... Enables Tou... Running Manual (Trig... Local Syste...
Extended
Standard

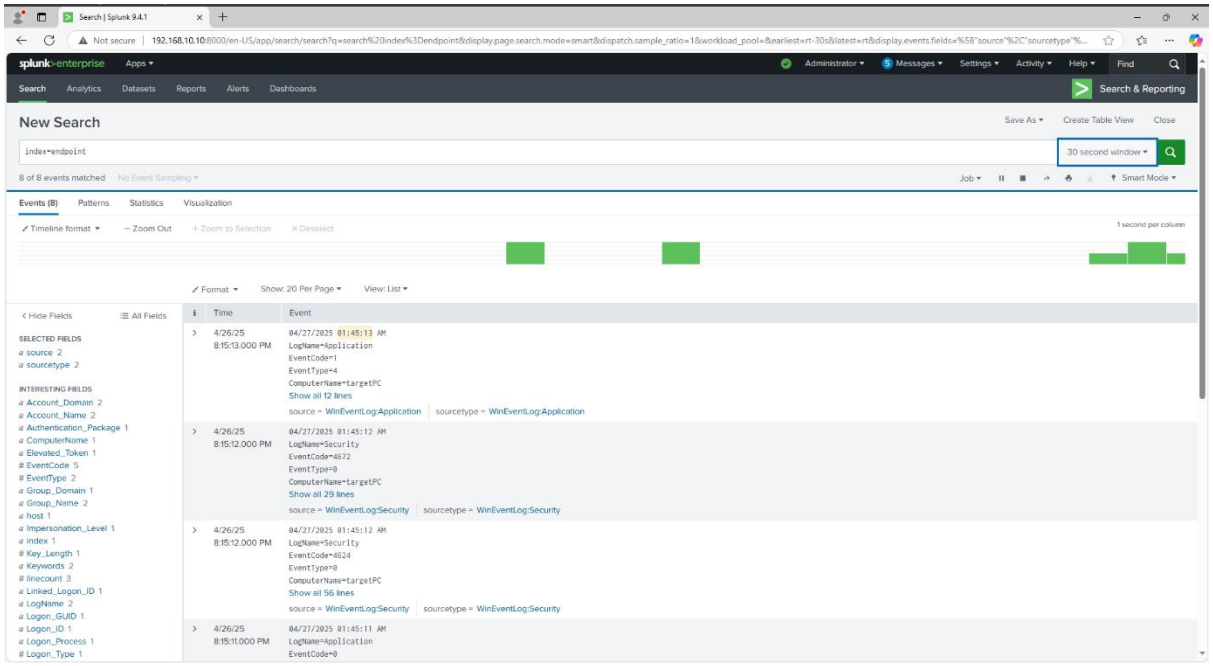

Home
Not secure | 192.168.10.10:8000/en-US/app/launcher/home
splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Apps
Find more apps
Manage
Search apps by name...
Search & Reporting
Audit Trail
Splunk Secure Gateway
Upgrade Readiness App
Hello, Administrator
Home page settings
Bookmarks
Dashboard
Search history
Recently viewed
Created by you
Shared with you
My bookmarks (0)
Add bookmark
Shared with my organization (0)
Add bookmark
Splunk recommended (13)

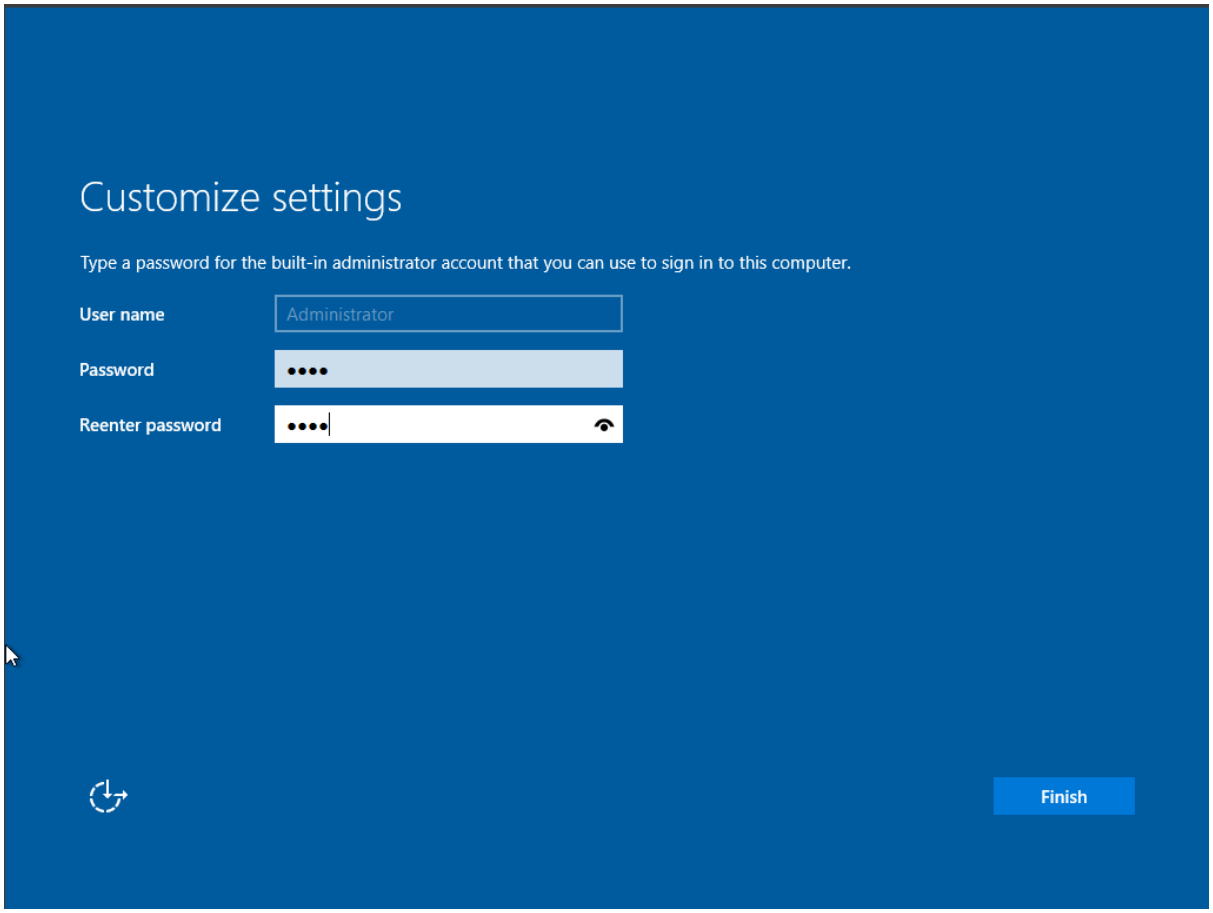

Not secure | 192.168.10.10:8000/en-US/manager/launcher/data/indexes
splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Indexes
A repository for data in Splunk Enterprise. Indexes reside in flat files on the Splunk Enterprise instance known as the indexer. Learn more
New Index
15 Indexes
filter
20 per page
Name
Actions
Type
App
Current Size
Max Size
Event Count
Earliest Event
Latest Event
Home Path
Frozen Path
Status
_audit Edit Delete Disable Events system 1 MB 488.28 GB 0 $SPLUNK_DB/audit/db N/A Enabled
_configtracker Edit Delete Disable Events system 1 MB 488.28 GB 0 $SPLUNK_DB/_configtracker/db N/A Enabled
_dsappevent Edit Delete Disable Events SplunkDeploymentServerConfig 1 MB 488.28 GB 0 $SPLUNK_DB/_dsappevent/db N/A Enabled
_dsclient Edit Delete Disable Events SplunkDeploymentServerConfig 1 MB 488.28 GB 0 $SPLUNK_DB/_dsclient/db N/A Enabled
_dsphonehome Edit Delete Disable Events SplunkDeploymentServerConfig 1 MB 488.28 GB 0 $SPLUNK_DB/_dsphonehome/db N/A Enabled
_internal Edit Delete Disable Events system 1 MB 488.28 GB 0 $SPLUNK_DB/_internaldb/db N/A Enabled
_introspection Edit Delete Disable Events system 1 MB 488.28 GB 0 $SPLUNK_DB/_introspection/db N/A Enabled
_metrics Edit Delete Disable Metrics system 1 MB 488.28 GB 0 $SPLUNK_DB/_metrics/db N/A Enabled
_metrics_rollup Edit Delete Disable Metrics system 1 MB 488.28 GB 0 $SPLUNK_DB/_metrics_rollup/db N/A Enabled
_telemetry Edit Delete Disable Events system 1 MB 488.28 GB 0 $SPLUNK_DB/_telemetry/db N/A Enabled
_thefishbucket Edit Delete Disable Events system 1 MB 488.28 GB 0 $SPLUNK_DB/fishbucket/db N/A Enabled
history Edit Delete Disable Events system 1 MB 488.28 GB 0 $SPLUNK_DB/historydb/db N/A Enabled
main Edit Delete Disable Events system 1 MB 488.28 GB 0 $SPLUNK_DB/defaultdb/db N/A Enabled
splunklogger Edit Delete Enable Events system 0 B 488.28 GB 0 $SPLUNK_DB/splunklogger/db N/A Disabled
summary Edit Delete Disable Events system 1 MB 488.28 GB 0 $SPLUNK_DB/summarydb/db N/A Enabled
Task View

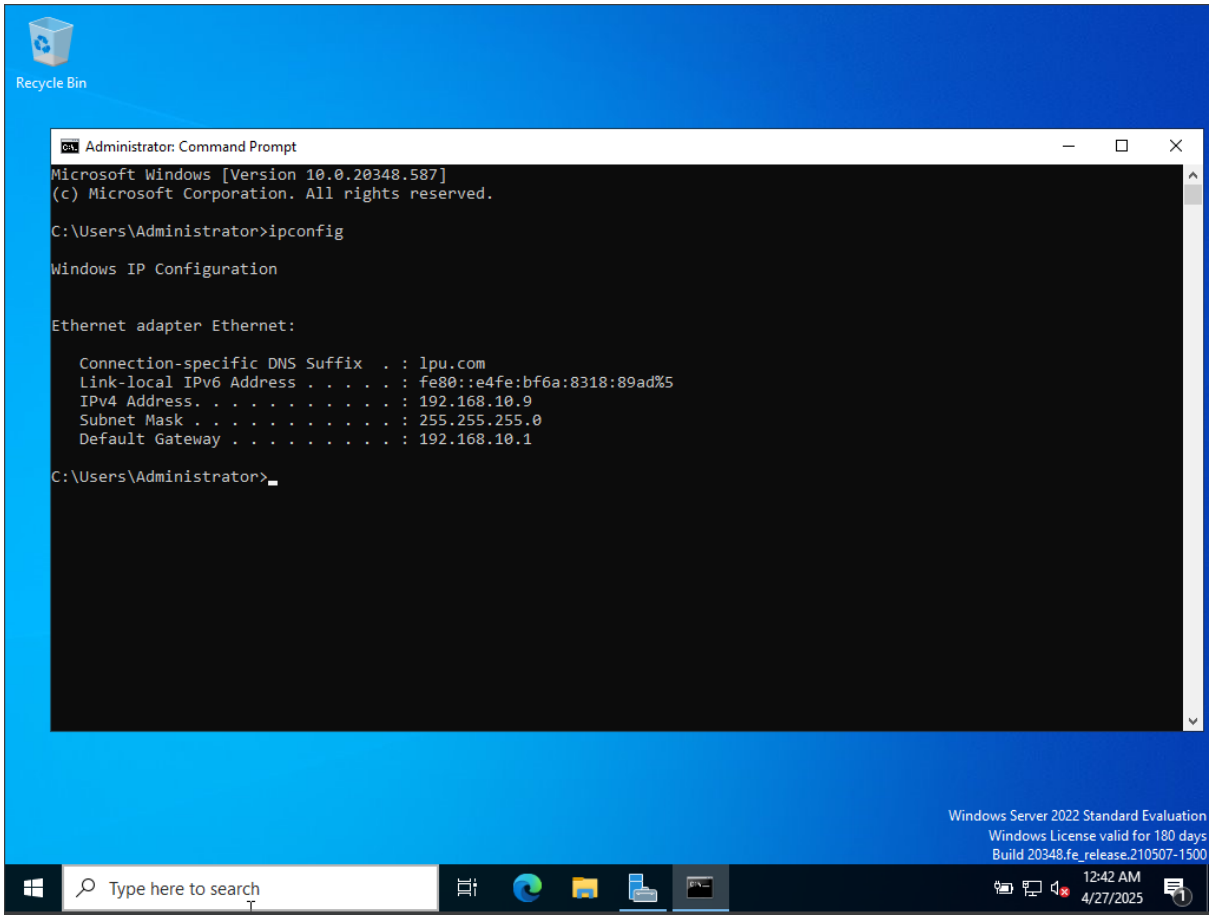

Manage Indexes | Splunk 9.4.1
Not secure | 192.168.10.10:8000/en-US/manager/launcher/data/indexes
Indexes
New Index
General Settings
Index Name
endpoint
Index Data Type
Events
Metrics
Home Path
optional
Cold Path
optional
Thawed Path
optional
Data Integrity Check
Enable
Disable
Max Size of Entire Index
500
GB
Max Size of Hot/Warm/Cold Bucket
auto
GB
Frozen Path
optional
App
Search & Reporting
Storage Optimization
Tsidx Retention Policy
Enable Reduction
Disable Reduction
Save
Cancel

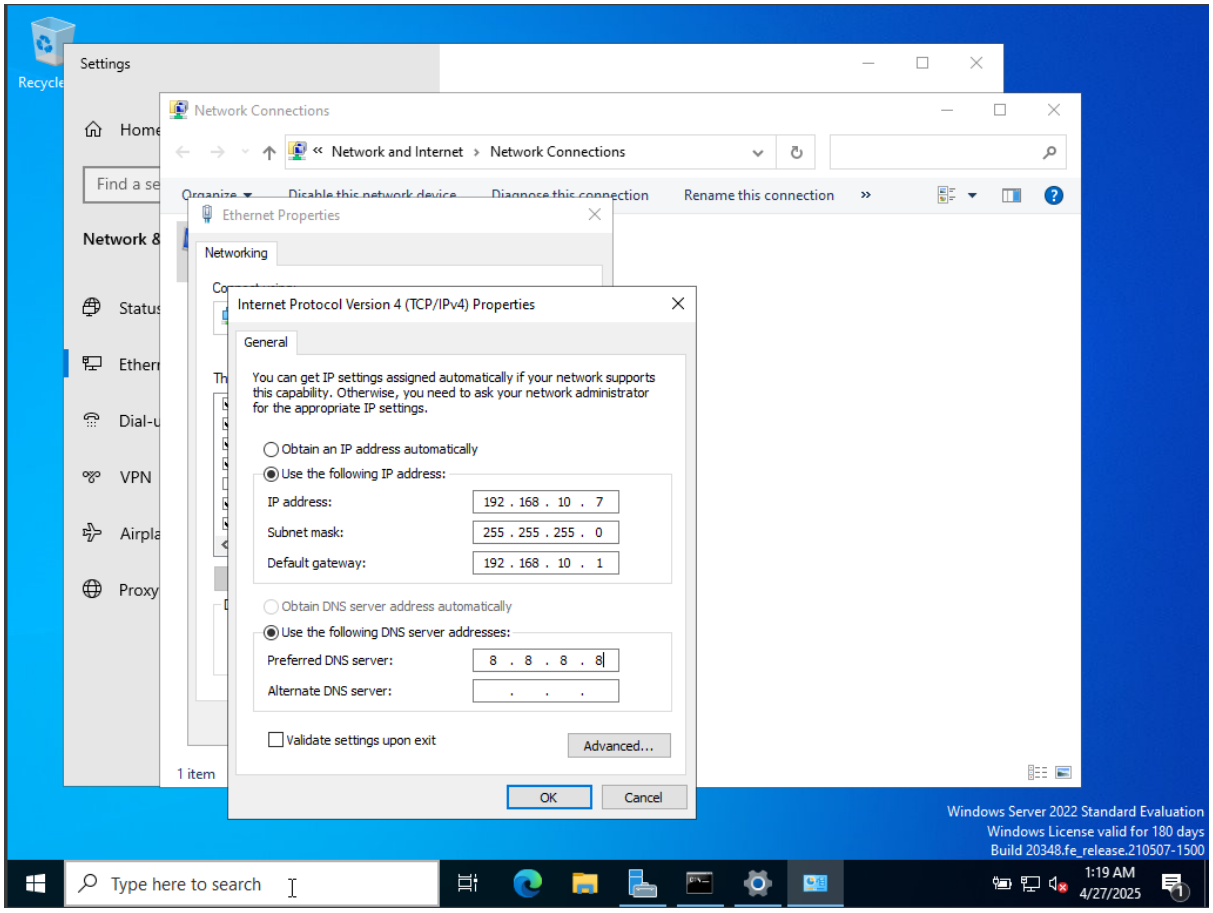

Settings | Splunk
Not secure | 192.168.10.10:8000/en-US/manager/launcher/forwardreceive
splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Forwarding and receiving
Forward data
Set up forwarding between two or more Splunk instances.
Type
Actions
Forwarding defaults
Configure forwarding
+ Add new
Receive data
Configure this instance to receive data forwarded from other instances.
Type
Actions
Configure receiving
+ Add new

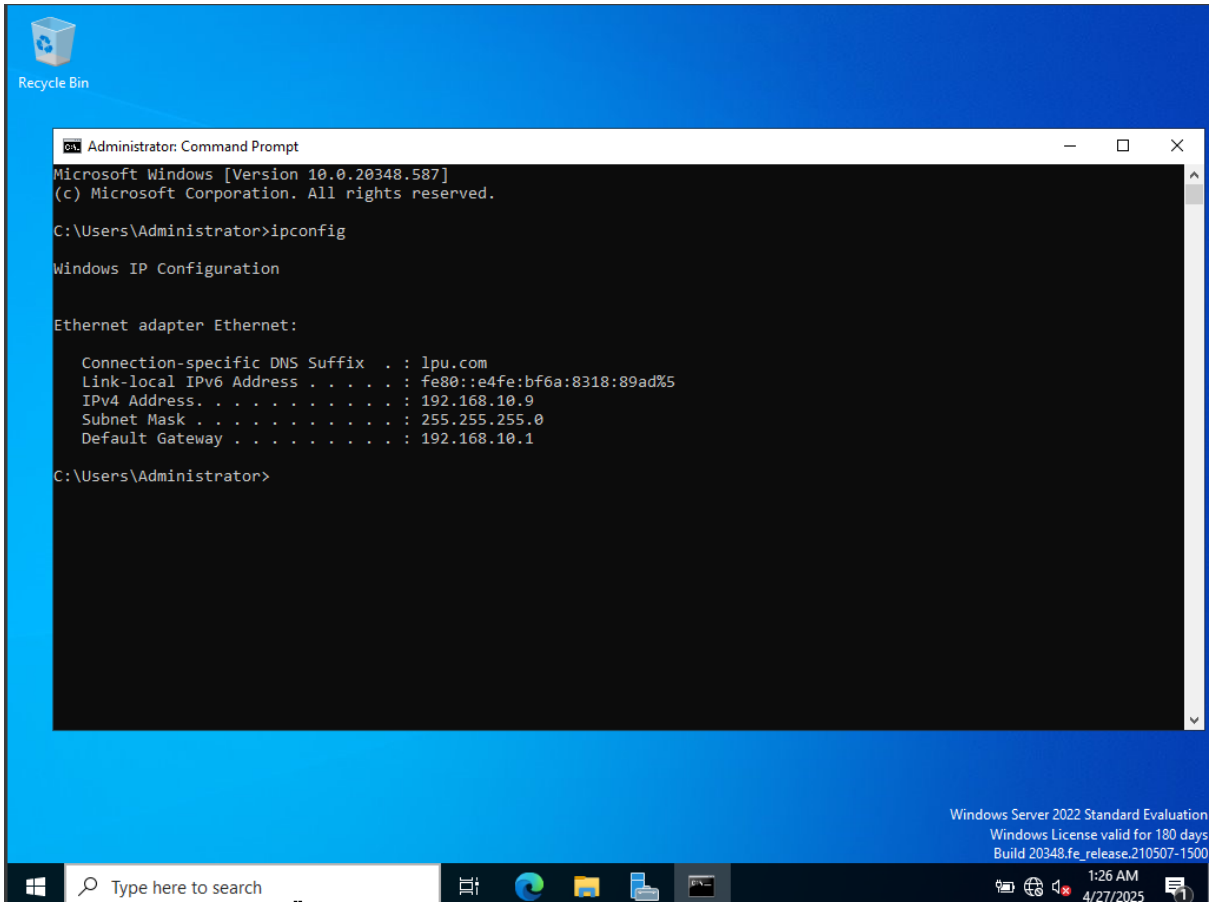

Settings | Splunk
Not secure | 192.168.10.10:8000/en-US/manager/launcher/data/inputs/tcp/cooked/_new?action=edit&ns=launcher
splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Add new
Forwarding and receiving » Receive data » Add new
Configure receiving
Set up this Splunk instance to receive data from forwarder(s).
Listen on this port *
For example, 9997 will receive data on TCP port 9997.
Cancel
Save

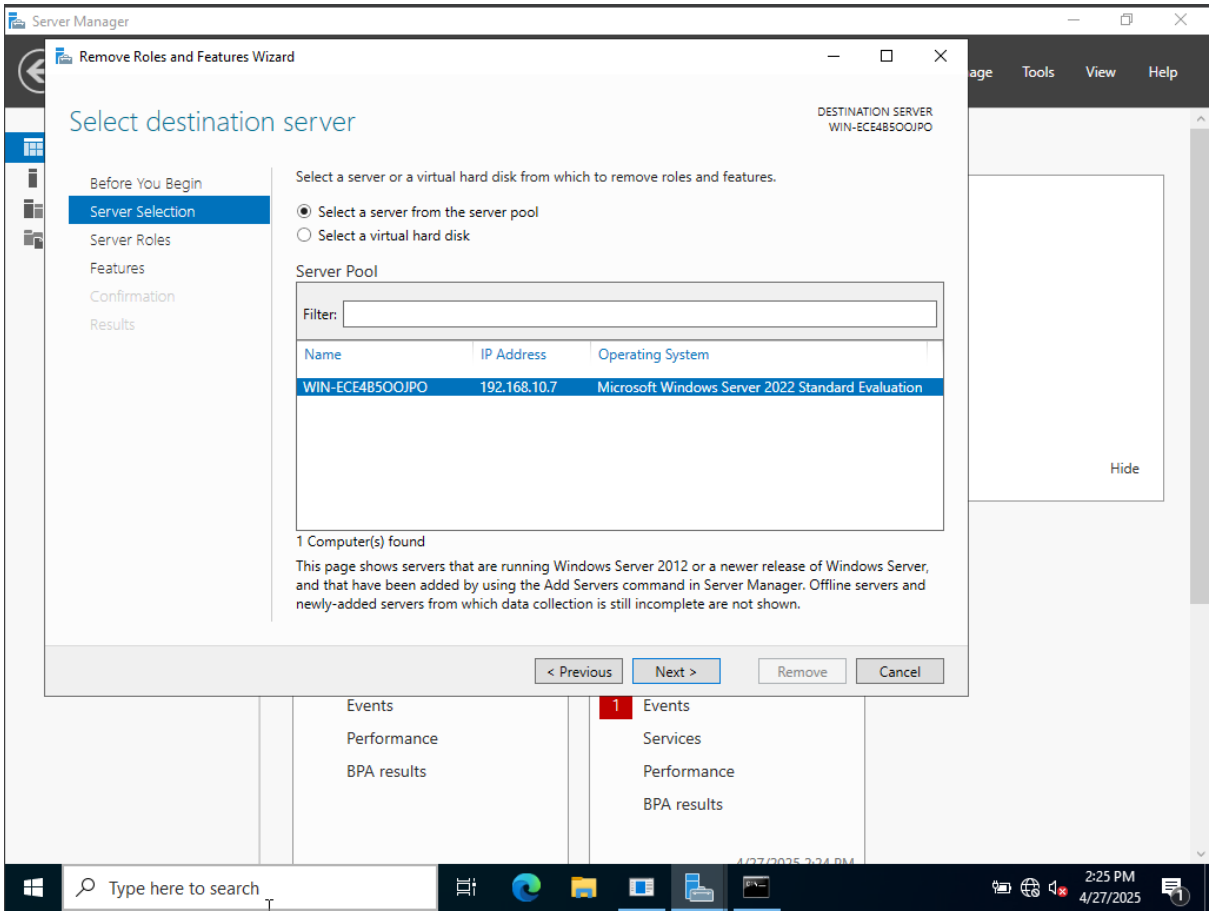

Search | Splunk 9.4.1
Not secure | 192.168.10.10:8000/en-US/app/search/search?q=search%20index%3Dendpoint&display.page.search.mode=smart&dispatch.sample_ratio=1&workload_pool=&earliest=rt-30s&latest=rt&display.events.fields=%5B"source"%2C"sourcetype"%...
splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
New Search
Save As
Create Table View
Close
index=endpoint
30 second window
8 of 8 events matched
No Event Sampling
Job
Smart Mode
Events (8)
Patterns
Statistics
Visualization
Timeline format
Zoom Out
Zoom to Selection
Deselect
1 second per column
Format
Show: 20 Per Page
View: List
Hide Fields
All Fields
SELECTED FIELDS
source 2
sourcetype 2
INTERESTING FIELDS
Account_Domain 2
Account_Name 2
Authentication_Package 1
ComputerName 1
Elevated_Token 1
EventCode 5
EventType 2
Group_Domain 1
Group_Name 2
host 1
Impersonation_Level 1
index 1
Key_Length 1
Keywords 2
linecount 3
Linked_Logon_ID 1
LogName 2
Logon_GUID 1
Logon_ID 1
Logon_Process 1
Logon_Type 1
Time
Event
4/26/25 8:15:13.000 PM
04/27/2025 01:45:13 AM
LogName=Application
EventCode=1
EventType=4
ComputerName=targetPC
Show all 12 lines
source = WinEventLog:Application
sourcetype = WinEventLog:Application
4/26/25 8:15:12.000 PM
04/27/2025 01:45:12 AM
LogName=Security
EventCode=4672
EventType=0
ComputerName=targetPC
Show all 29 lines
source = WinEventLog:Security
sourcetype = WinEventLog:Security
4/26/25 8:15:12.000 PM
04/27/2025 01:45:12 AM
LogName=Security
EventCode=4624
EventType=0
ComputerName=targetPC
Show all 56 lines
source = WinEventLog:Security
sourcetype = WinEventLog:Security
4/26/25 8:15:11.000 PM
04/27/2025 01:45:11 AM
LogName=Application
EventCode=0

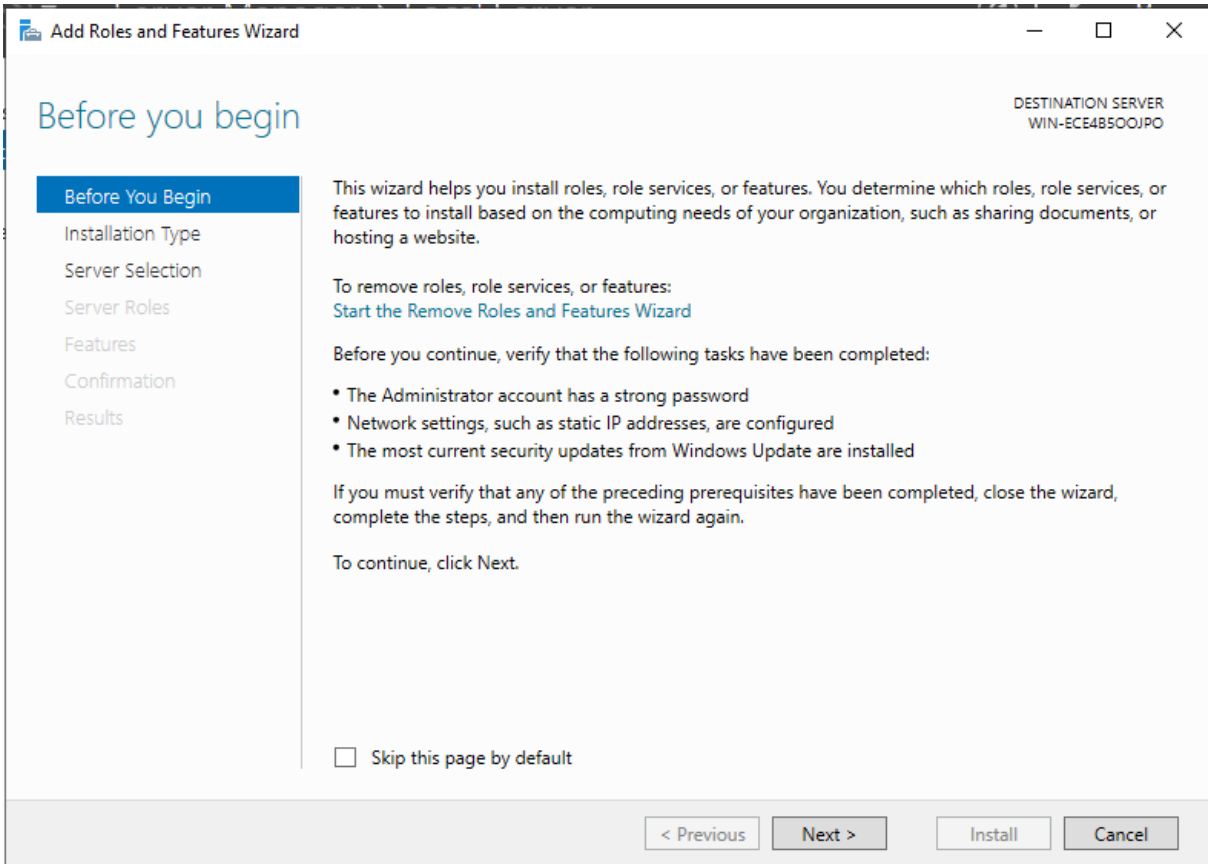

Customize settings
Type a password for the built-in administrator account that you can use to sign in to this computer.
User name
Administrator
Password
Reenter password
Finish

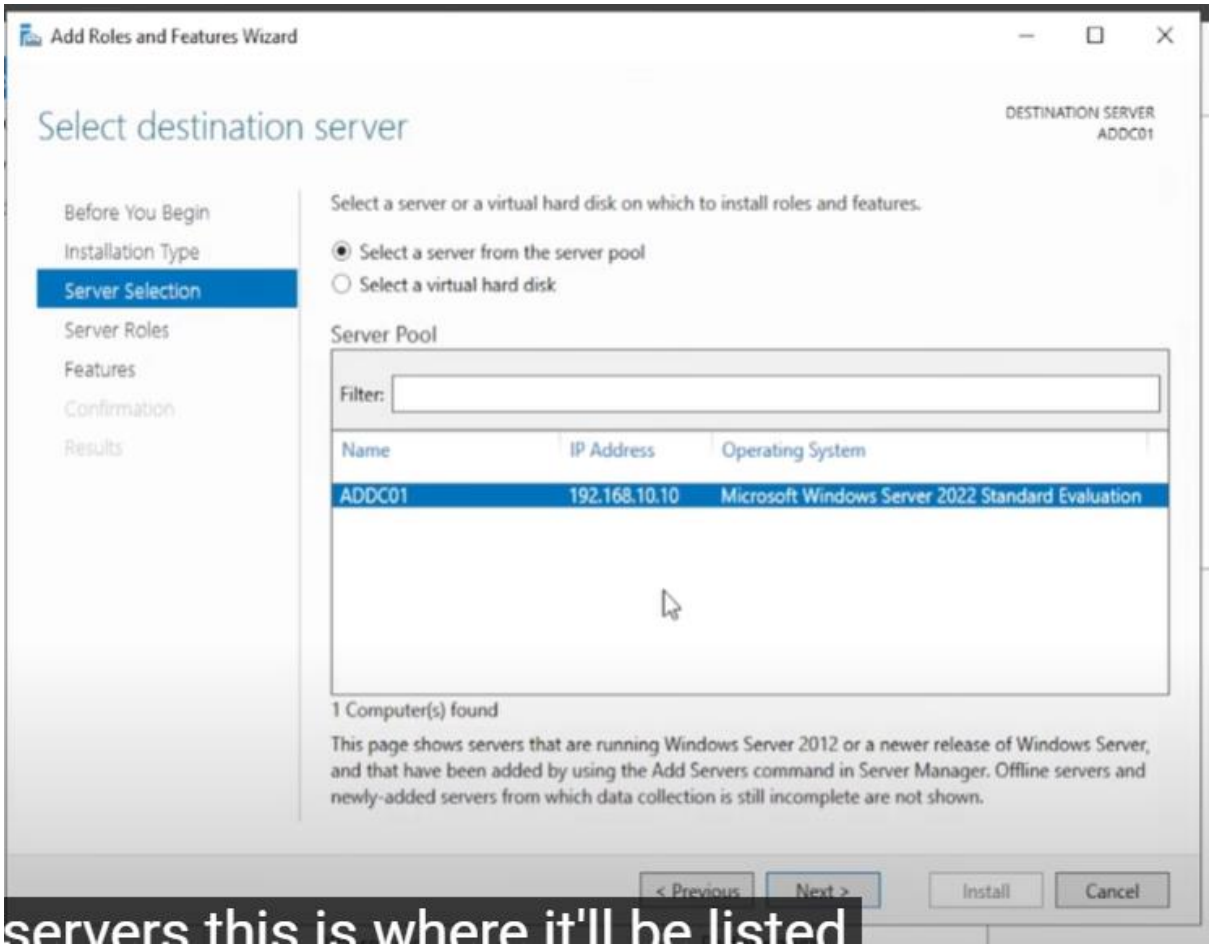

Recycle Bin
Administrator: Command Prompt
Microsoft Windows [Version 10.0.20348.587]
(c) Microsoft Corporation. All rights reserved.
C:\Users\Administrator>ipconfig
Windows IP Configuration
Ethernet adapter Ethernet:
Connection-specific DNS Suffix . : lpu.com
Link-local IPv6 Address . . . . . : fe80::e4fe:bf6a:8318:89ad%5
IPv4 Address. . . . . : 192.168.10.9
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.10.1
C:\Users\Administrator>
Windows Server 2022 Standard Evaluation
Windows License valid for 180 days
Build 20348.fe_release.210507-1500
Type here to search
12:42 AM
4/27/2025


Settings
Network Connections
Network and Internet › Network Connections
Rename this connection
Ethernet Properties
Networking
Internet Protocol Version 4 (TCP/IPv4) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address: 192 . 168 . 10 . 7
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 192 . 168 . 10 . 1
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server: 8 . 8 . 8 . 8
Alternate DNS server:
Validate settings upon exit
Advanced...
OK
Cancel
1 item
Windows Server 2022 Standard Evaluation
Windows License valid for 180 days
Build 20348.fe_release.210507-1500
Type here to search
1:19 AM
4/27/2025

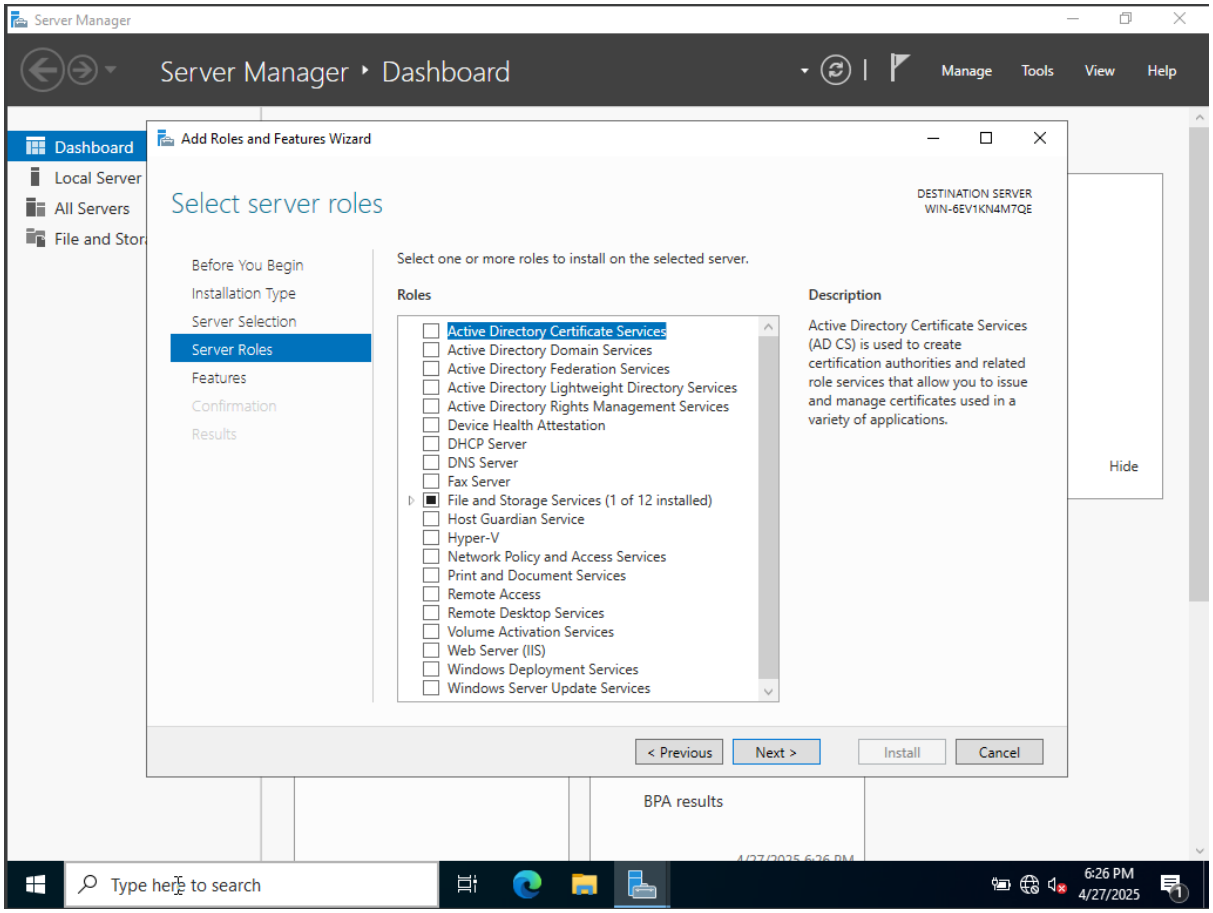

Recycle Bin
Administrator: Command Prompt
Microsoft Windows [Version 10.0.20348.587]
(c) Microsoft Corporation. All rights reserved.
C:\Users\Administrator>ipconfig
Windows IP Configuration
Ethernet adapter Ethernet:
Connection-specific DNS Suffix . : lpu.com
Link-local IPv6 Address . . . . . : fe80::e4fe:bf6a:8318:89ad%5
IPv4 Address. . . . . : 192.168.10.9
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.10.1
C:\Users\Administrator>
Windows Server 2022 Standard Evaluation
Windows License valid for 180 days
Build 20348.fe_release.210507-1500
Type here to search
1:26 AM
4/27/2025

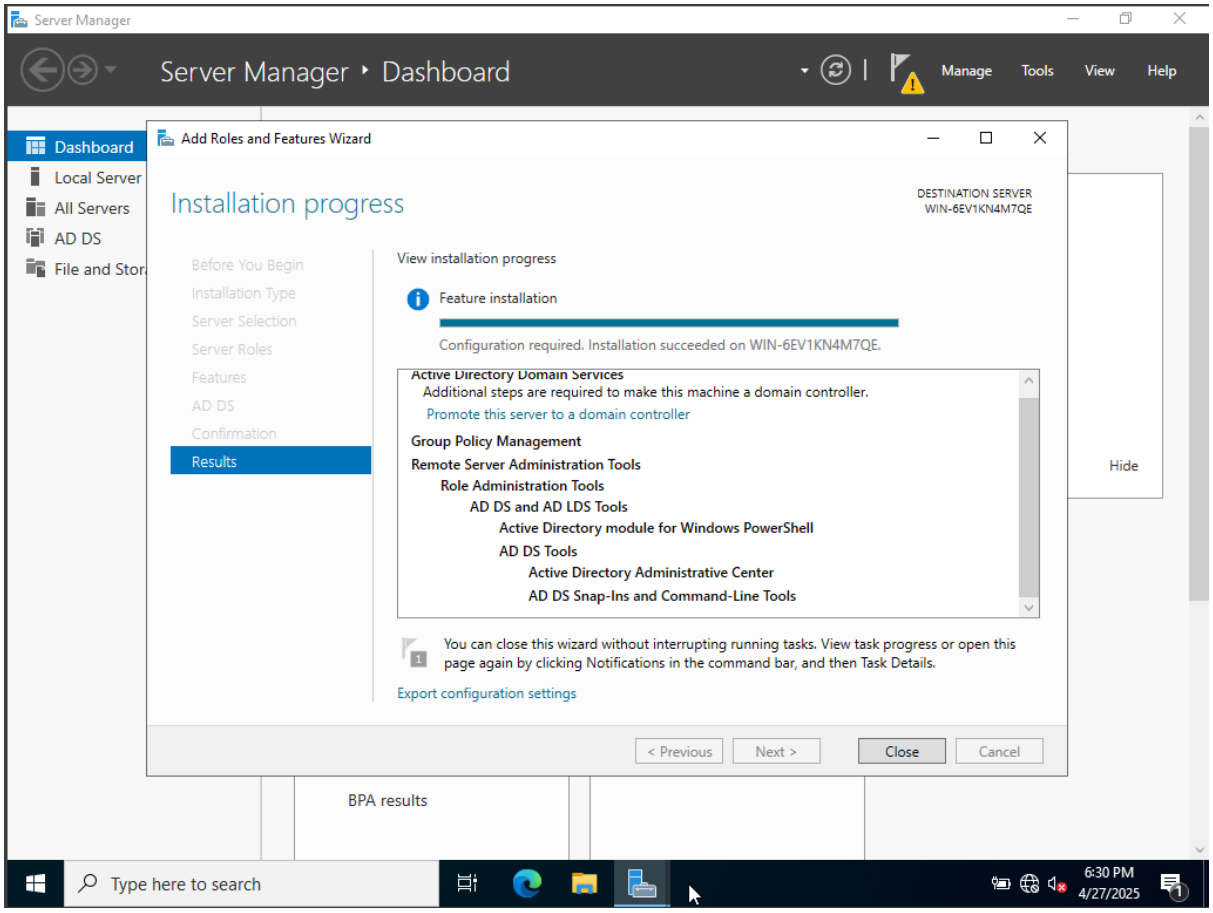

Server Manager
Remove Roles and Features Wizard
Select destination server
DESTINATION SERVER
WIN-ECE4B5OOJPO
Before You Begin
Server Selection
Server Roles
Features
Confirmation
Results
Select a server or a virtual hard disk from which to remove roles and features.
Select a server from the server pool
Select a virtual hard disk
Server Pool
Filter:
Name
IP Address
Operating System
WIN-ECE4B5OOJPO
192.168.10.7
Microsoft Windows Server 2022 Standard Evaluation
1 Computer(s) found
This page shows servers that are running Windows Server 2012 or a newer release of Windows Server, and that have been added by using the Add Servers command in Server Manager. Offline servers and newly-added servers from which data collection is still incomplete are not shown.
< Previous
Next >
Remove
Cancel
Tools
View
Help
Hide
Events
Performance
BPA results
Services
Type here to search
2:25 PM
4/27/2025

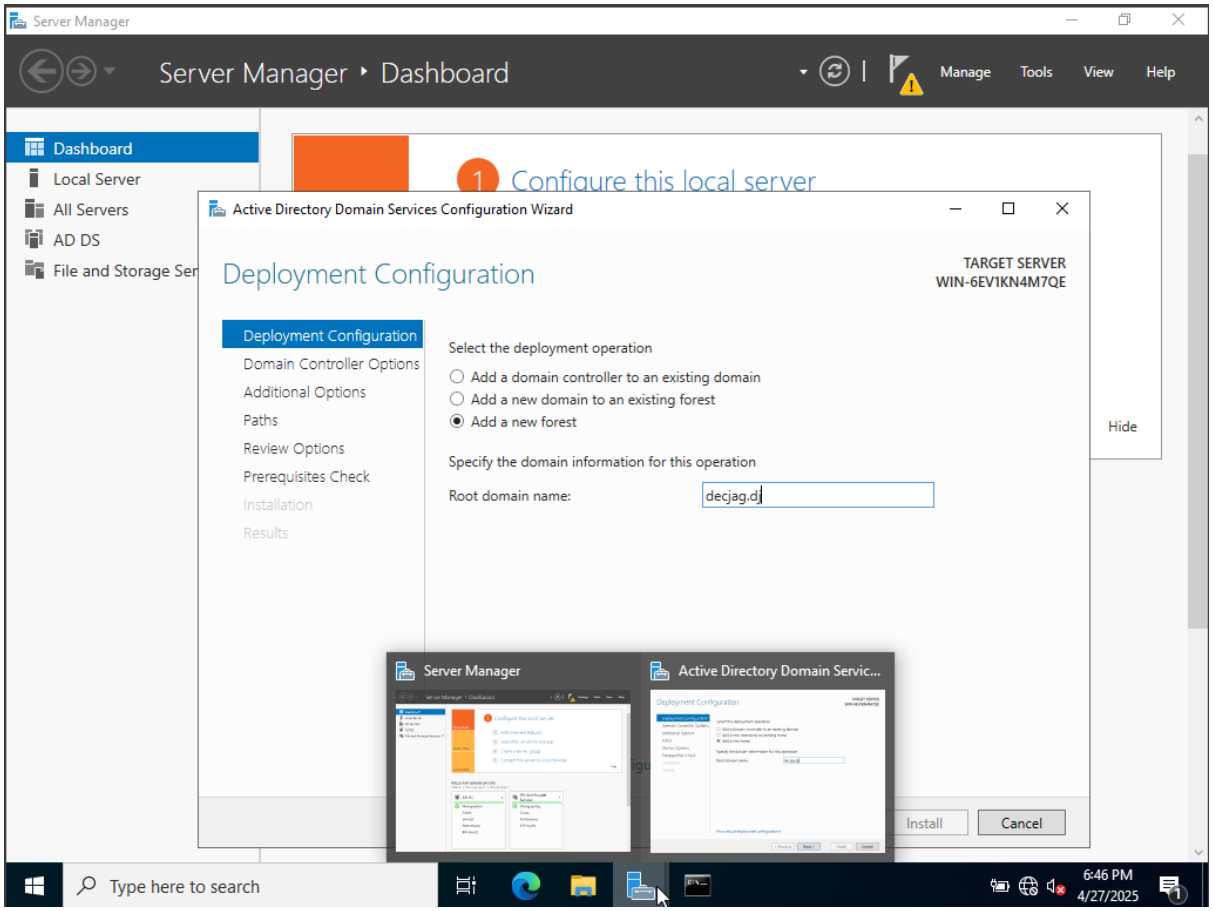

Add Roles and Features Wizard
Before you begin
DESTINATION SERVER
WIN-ECE4B5OOJPO
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
This wizard helps you install roles, role services, or features. You determine which roles, role services, or features to install based on the computing needs of your organization, such as sharing documents, or hosting a website.
To remove roles, role services, or features:
Start the Remove Roles and Features Wizard
Before you continue, verify that the following tasks have been completed:
• The Administrator account has a strong password
• Network settings, such as static IP addresses, are configured
• The most current security updates from Windows Update are installed
If you must verify that any of the preceding prerequisites have been completed, close the wizard, complete the steps, and then run the wizard again.
To continue, click Next.
Skip this page by default
< Previous
Next >
Install
Cancel

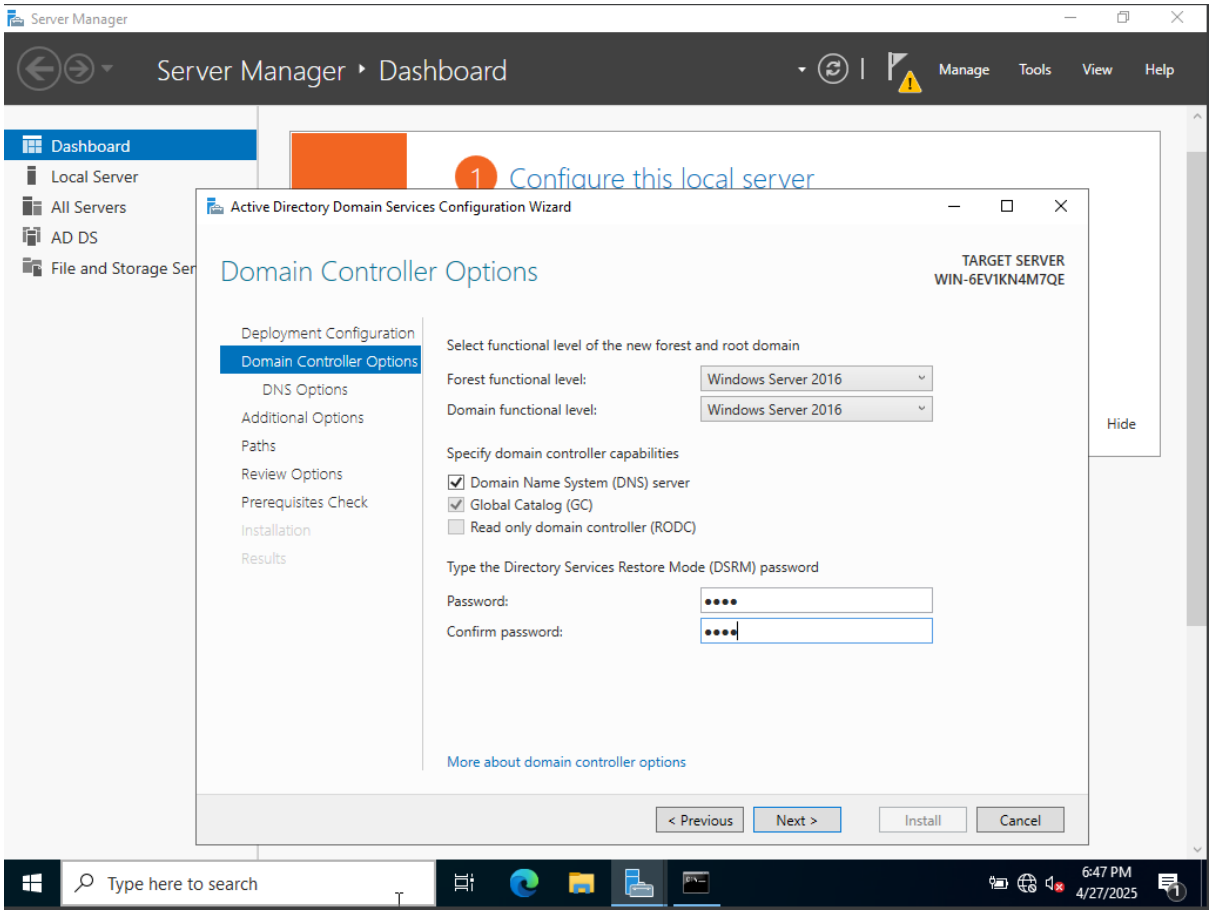


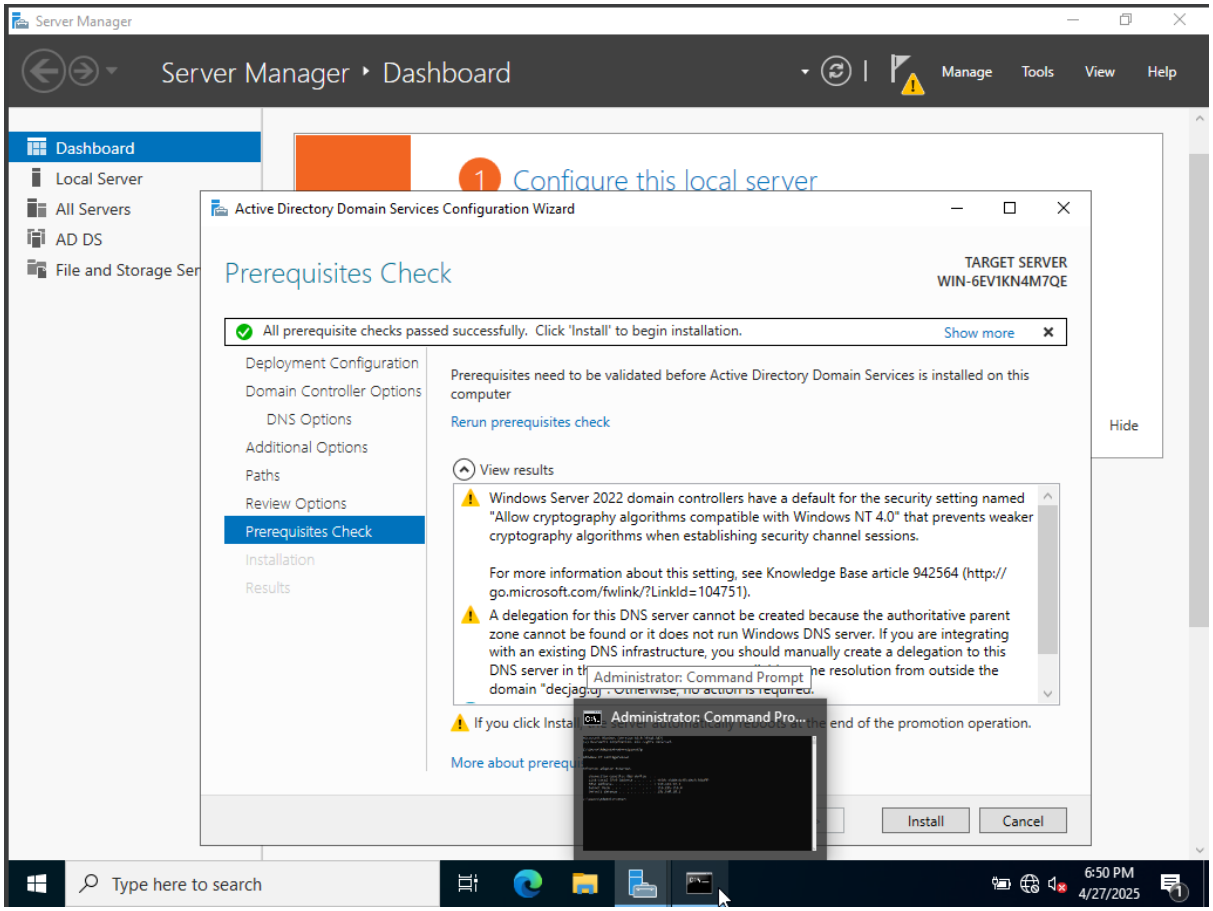
servers this is where it'll be listed

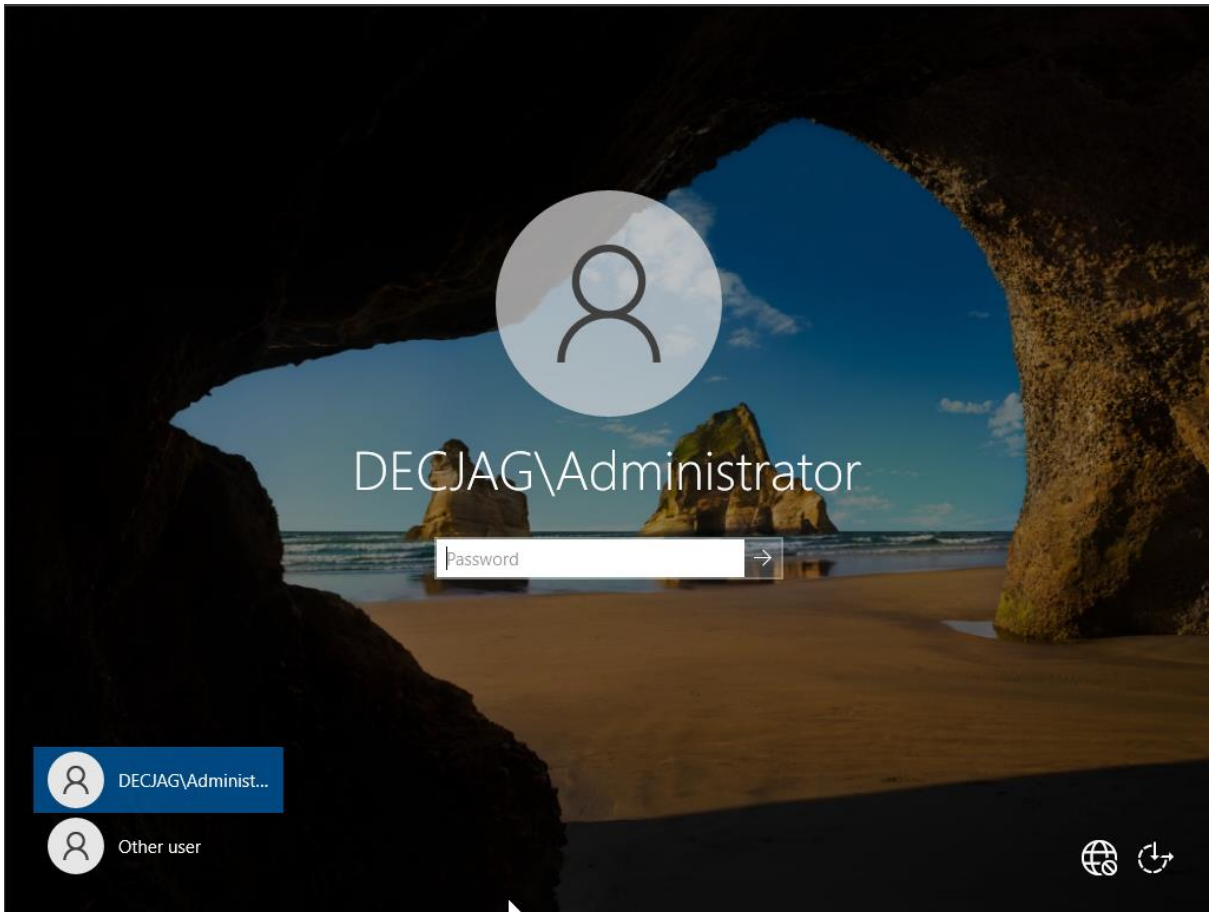


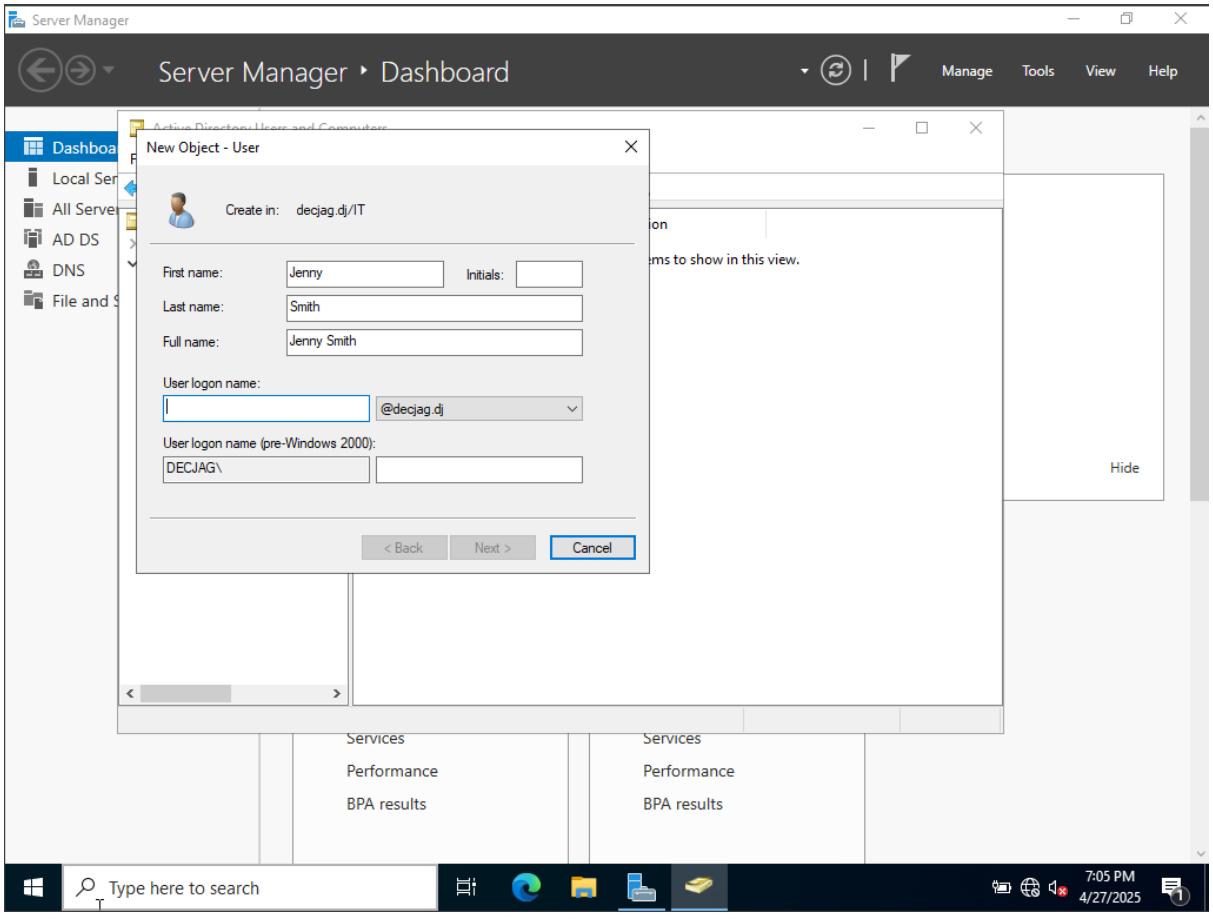

Server Manager
Server Manager • Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
AD DS
File and Stor
Add Roles and Features Wizard
Installation progress
DESTINATION SERVER
WIN-6EV1KN4M7QE
Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD DS
Confirmation
Results
View installation progress
Feature installation
Configuration required. Installation succeeded on WIN-6EV1KN4M7QE.
Active Directory Domain Services
Additional steps are required to make this machine a domain controller.
Promote this server to a domain controller
Group Policy Management
Remote Server Administration Tools
Role Administration Tools
AD DS and AD LDS Tools
Active Directory module for Windows PowerShell
AD DS Tools
Active Directory Administrative Center
AD DS Snap-Ins and Command-Line Tools
You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.
Export configuration settings
< Previous
Next >
Close
Cancel
Hide
BPA results
Type here to search
6:30 PM
4/27/2025

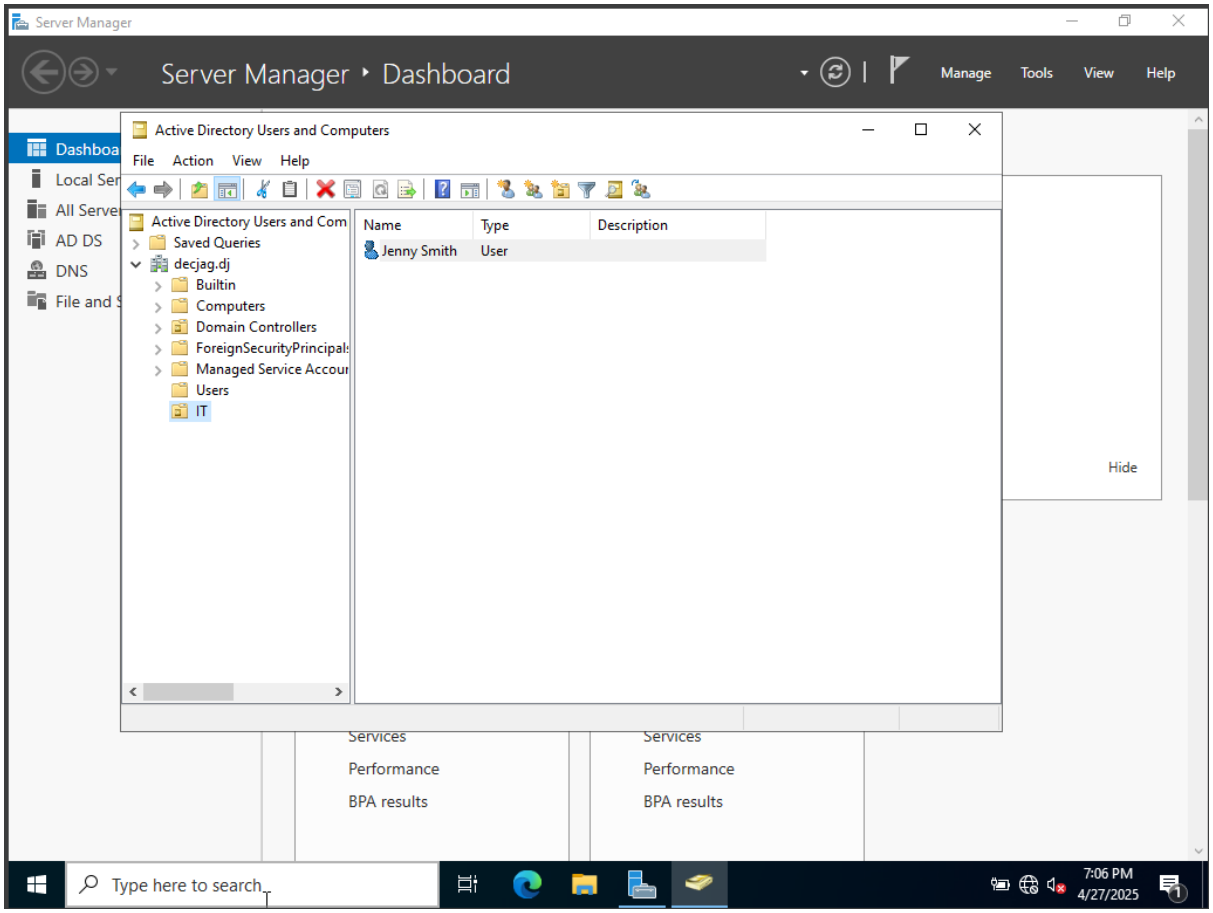

Server Manager
Server Manager • Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
AD DS
File and Storage Ser
Configure this local server
Active Directory Domain Services Configuration Wizard
Deployment Configuration
TARGET SERVER
WIN-6EV1KN4M7QE
Deployment Configuration
Domain Controller 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
Root domain name:
decjag.dj
Server Manager
Active Directory Domain Servic...
Install
Cancel
Hide
Type here to search
6:46 PM
4/27/2025

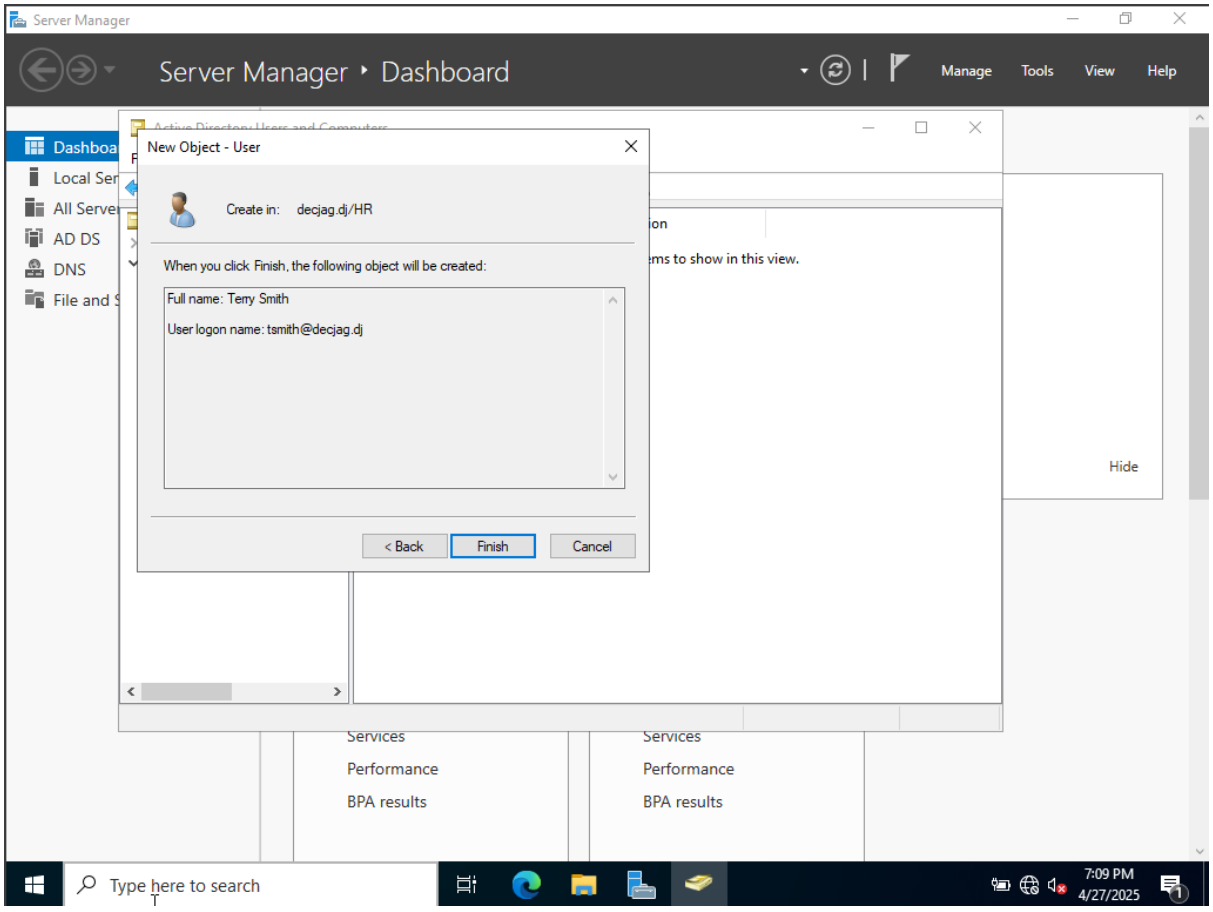

Server Manager
Server Manager ‣ Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
AD DS
File and Storage Ser
Configure this local server
Active Directory Domain Services Configuration Wizard
Domain Controller Options
TARGET SERVER
WIN-6EV1KN4M7QE
Deployment Configuration
Domain Controller 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
Hide
Type here to search
6:47 PM
4/27/2025

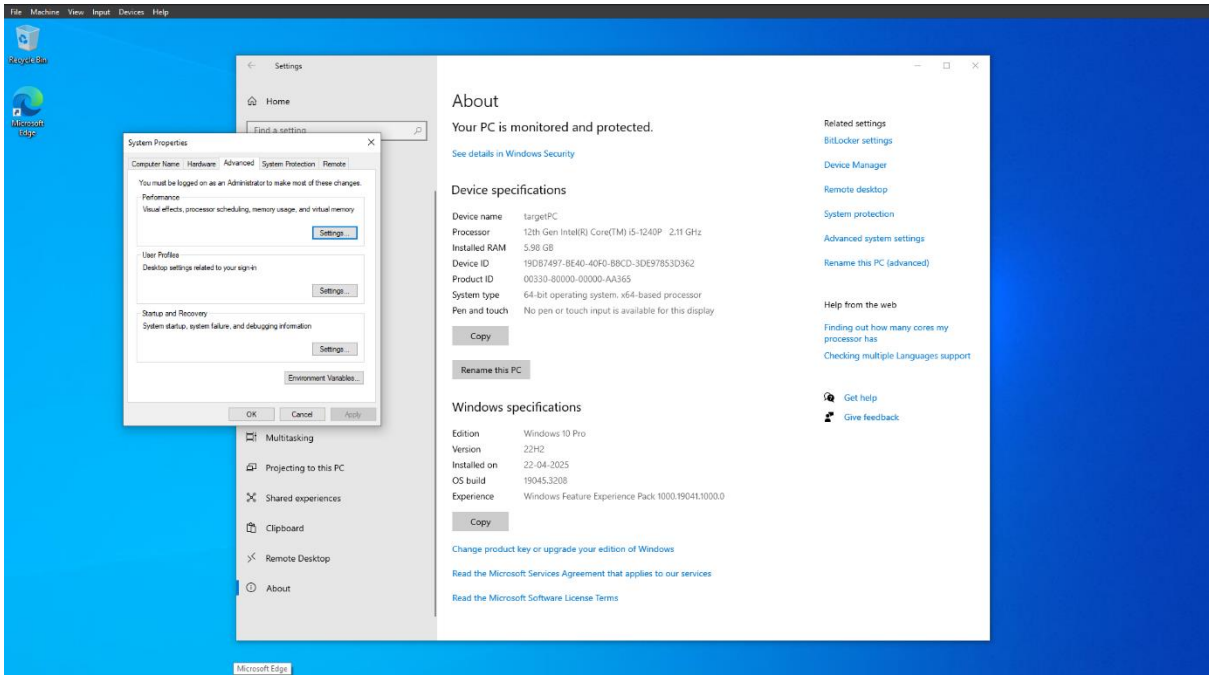

Server Manager
Server Manager ‣ Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
AD DS
File and Storage Ser
Configure this local server
Active Directory Domain Services Configuration Wizard
Prerequisites Check
TARGET SERVER
WIN-6EV1KN4M7QE
All prerequisite checks passed successfully. Click 'Install' to begin installation.
Show more
Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results
Prerequisites need to be validated before Active Directory Domain Services is installed on this computer
Rerun prerequisites check
View results
Windows Server 2022 domain controllers have a default for the security setting named "Allow cryptography algorithms compatible with Windows NT 4.0" that prevents weaker cryptography algorithms when establishing security channel sessions.
For more information about this setting, see Knowledge Base article 942564 (http://go.microsoft.com/fwlink/?LinkId=104751).
A delegation for this DNS server cannot be created because the authoritative parent zone cannot be found or it does not run Windows DNS server. If you are integrating with an existing DNS infrastructure, you should manually create a delegation to this DNS server in th
Administrator: Command Prompt
Administrator: Command Pro...
domain "decjag.ru". Otherwise, no action is required.
end of the promotion operation.
More about prerequ
Install
Cancel
Hide
Type here to search
6:50 PM
4/27/2025

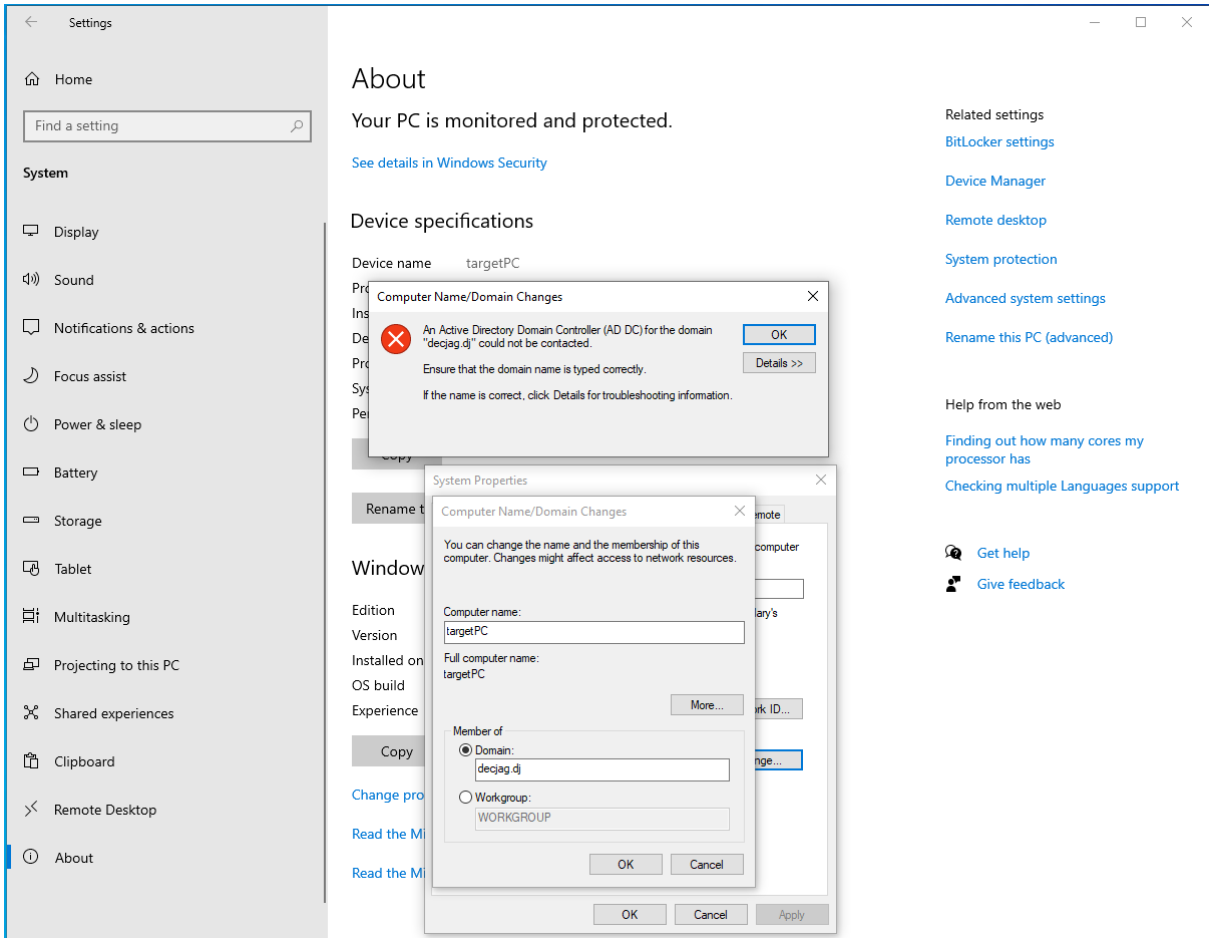

DECJAG\Administrator
Password
DECJAG\Administ...
Other user

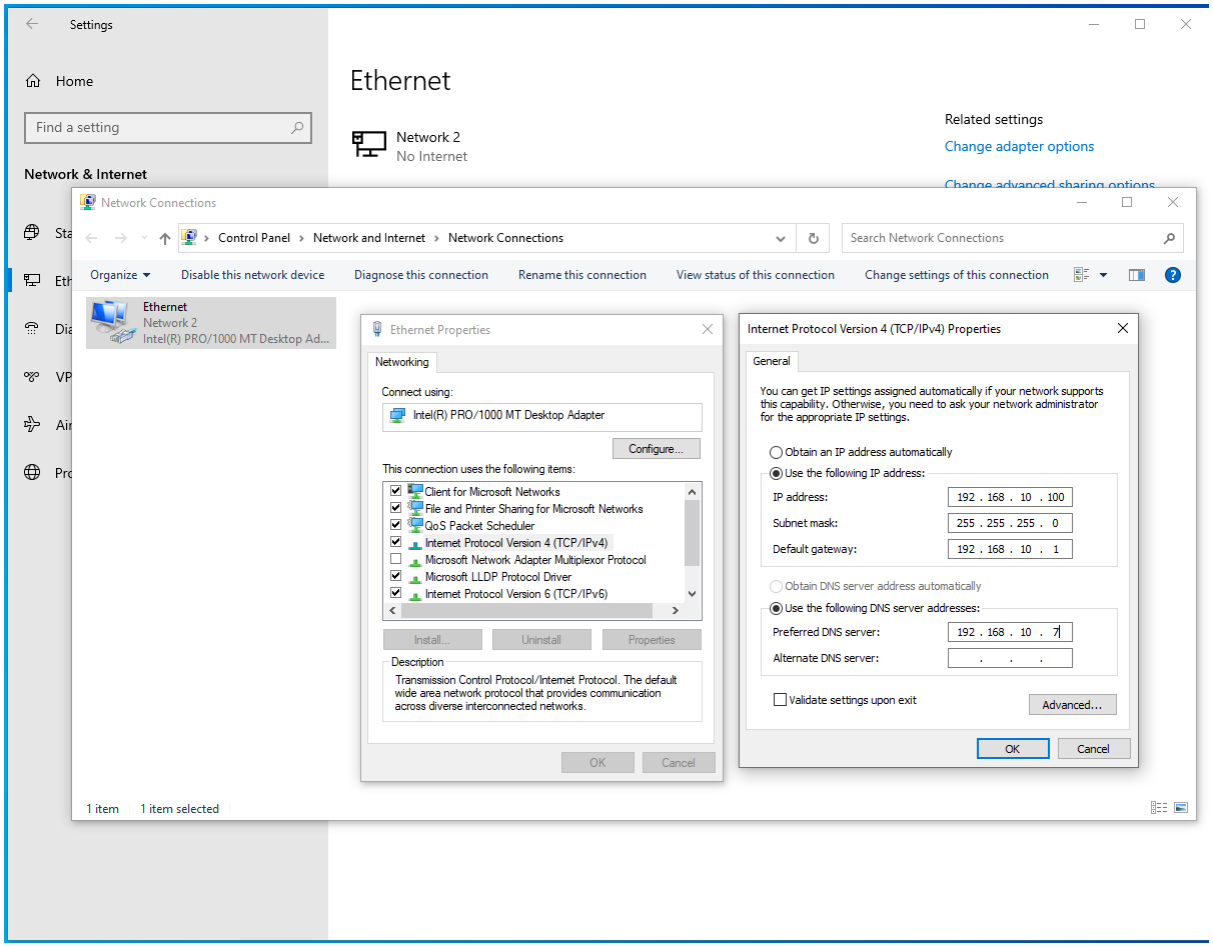

Server Manager
Server Manager ‣ Dashboard
Manage
Tools
View
Help
Dashboa
Local Ser
All Serve
AD DS
DNS
File and S
New Object - User
Create in: decjag.dj/IT
First name: Jenny
Initials:
Last name: Smith
Full name: Jenny Smith
User logon name:
@decjag.dj
User logon name (pre-Windows 2000):
DECJAG\
< Back
Next >
Cancel
Hide
Services
Performance
BPA results
Services
Performance
BPA results
Type here to search
7:05 PM
4/27/2025

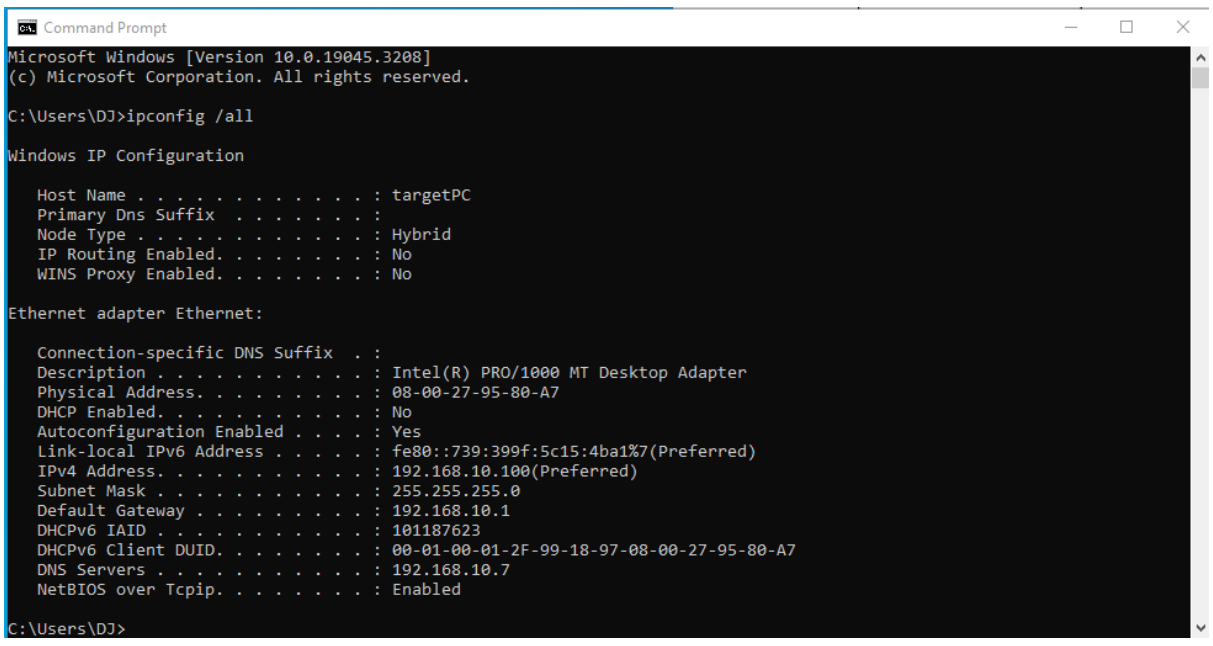

Server Manager
Server Manager • Dashboard
Manage
Tools
View
Help
Active Directory Users and Computers
File
Action
View
Help
Active Directory Users and Com
Saved Queries
decjag.dj
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Managed Service Accour
Users
IT
Name
Type
Description
Jenny Smith
User
Hide
Services
Performance
BPA results
Type here to search
7:06 PM
4/27/2025

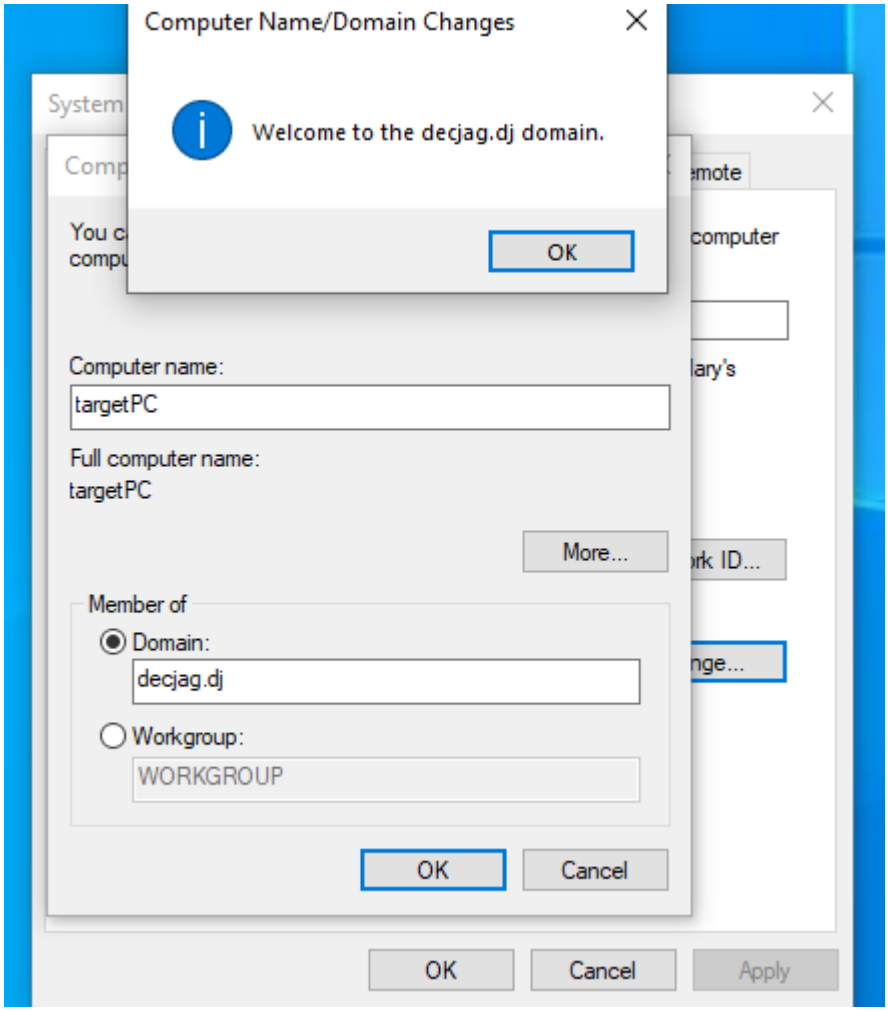

Server Manager
Server Manager • Dashboard
Manage
Tools
View
Help
New Object - User
Create in: decjag.dj/HR
When you click Finish, the following object will be created:
Full name: Terry Smith
User logon name: tsmith@decjag.dj
< Back
Finish
Cancel
Hide
Services
Performance
BPA results
Type here to search
7:09 PM
4/27/2025

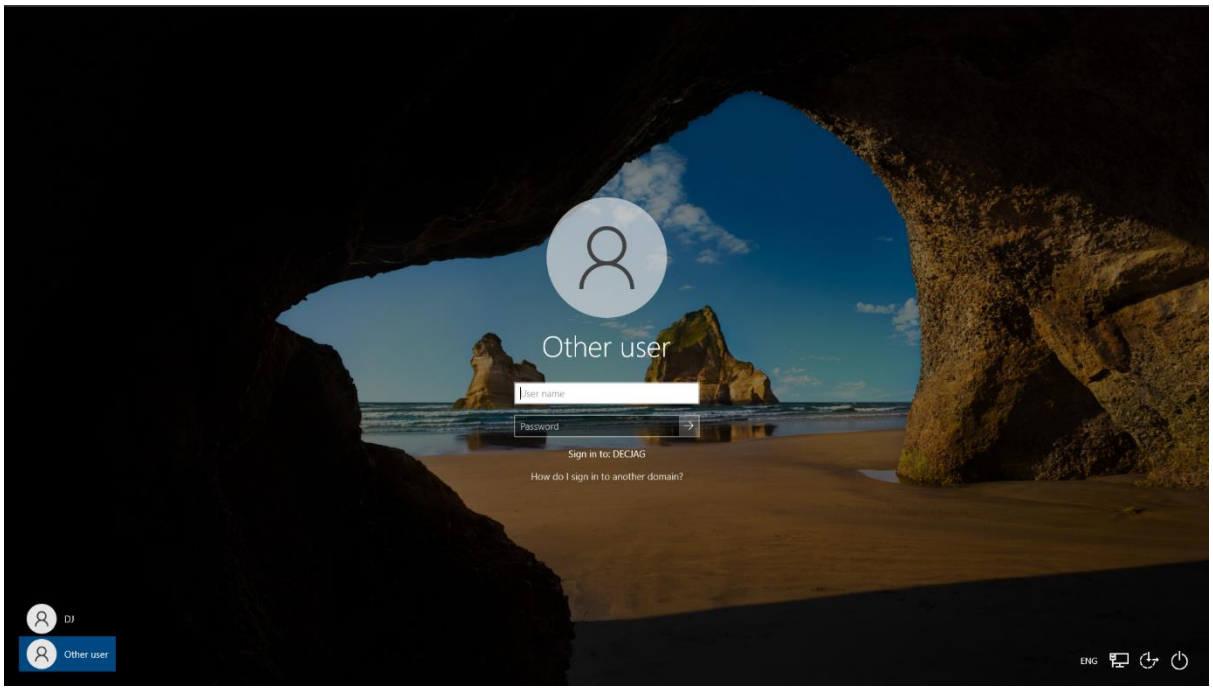

Settings
Home
About
Your PC is monitored and protected.
See details in Windows Security
Device specifications
Device name targetPC
Processor 12th Gen Intel(R) Core(TM) i5-1240P 2.11 GHz
Installed RAM 5.98 GB
Device ID 19DB7497-BE40-40F0-B8CD-3DE97853D362
Product ID 00330-80000-00000-AA365
System type 64-bit operating system, x64-based processor
Pen and touch No pen or touch input is available for this display
Copy
Rename this PC
Windows specifications
Edition Windows 10 Pro
Version 22H2
Installed on 22-04-2025
OS build 19045.3208
Experience Windows Feature Experience Pack 1000.19041.1000.0
Copy
Change product key or upgrade your edition of Windows
Read the Microsoft Services Agreement that applies to our services
Read the Microsoft Software License Terms
Related settings
BitLocker settings
Device Manager
Remote desktop
System protection
Advanced system settings
Rename this PC (advanced)
Help from the web
Finding out how many cores my processor has
Checking multiple Languages support
Get help
Give feedback
System Properties
Computer Name
Hardware
Advanced
System Protection
Remote
You must be logged on as an Administrator to make most of these changes.
Performance
Visual effects, processor scheduling, memory usage, and virtual memory
Settings...
User Profiles
Desktop settings related to your sign-in
Settings...
Startup and Recovery
System startup, system failure, and debugging information
Settings...
Environment Variables...
OK
Cancel
Apply
Multitasking
Projecting to this PC
Shared experiences
Clipboard
Remote Desktop
About
Microsoft Edge

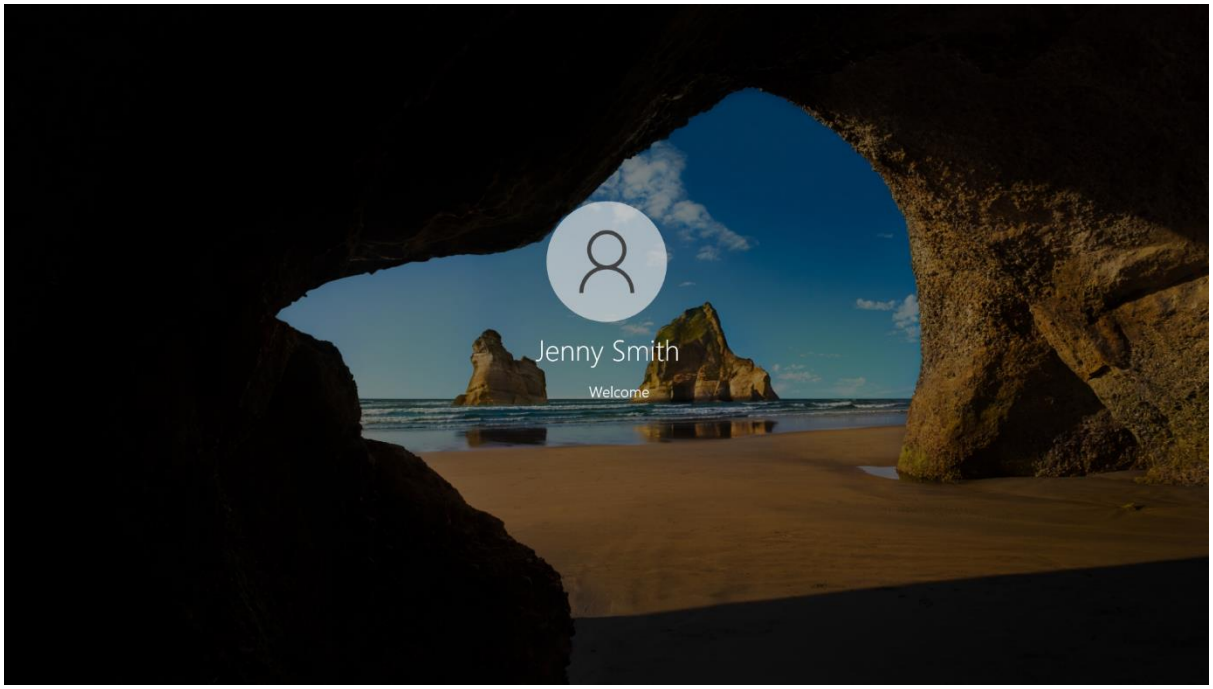

Settings
Home
Find a setting
System
Display
Sound
Notifications & actions
Focus assist
Power & sleep
Battery
Storage
Tablet
Multitasking
Projecting to this PC
Shared experiences
Clipboard
Remote Desktop
About
About
Your PC is monitored and protected.
See details in Windows Security
Device specifications
Device name targetPC
Computer Name/Domain Changes
An Active Directory Domain Controller (AD DC) for the domain "decjag.dj" could not be contacted.
Ensure that the domain name is typed correctly.
If the name is correct, click Details for troubleshooting information.
OK
Details >>
System Properties
Computer Name/Domain Changes
You can change the name and the membership of this computer. Changes might affect access to network resources.
Computer name:
targetPC
Full computer name:
targetPC
More...
Member of
Domain:
decjag.dj
Workgroup:
WORKGROUP
OK
Cancel
OK
Cancel
Apply
Related settings
BitLocker settings
Device Manager
Remote desktop
System protection
Advanced system settings
Rename this PC (advanced)
Help from the web
Finding out how many cores my processor has
Checking multiple Languages support
Get help
Give feedback


Settings
Home
Find a setting
Network & Internet
Ethernet
Network 2
No Internet
Related settings
Change adapter options
Network Connections
Control Panel › Network and Internet › Network Connections
Search Network Connections
Organize
Disable this network device
Diagnose this connection
Rename this connection
View status of this connection
Change settings of this connection
Ethernet
Network 2
Intel(R) PRO/1000 MT Desktop Ad...
Ethernet Properties
Networking
Connect using:
Intel(R) PRO/1000 MT Desktop Adapter
Configure...
This connection uses the following items:
Client for Microsoft Networks
File and Printer Sharing for Microsoft Networks
QoS Packet Scheduler
Internet Protocol Version 4 (TCP/IPv4)
Microsoft Network Adapter Multiplexor Protocol
Microsoft LLDP Protocol Driver
Internet Protocol Version 6 (TCP/IPv6)
Install...
Uninstall
Properties
Description
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.
OK
Cancel
Internet Protocol Version 4 (TCP/IPv4) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address: 192 . 168 . 10 . 100
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 192 . 168 . 10 . 1
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server: 192 . 168 . 10 . 7
Alternate DNS server:
Validate settings upon exit
Advanced...
OK
Cancel
1 item
1 item selected


Command Prompt
Microsoft Windows [Version 10.0.19045.3208]
(c) Microsoft Corporation. All rights reserved.
C:\Users\DJ>ipconfig /all
Windows IP Configuration
Host Name . . . . . : targetPC
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
Ethernet adapter Ethernet:
Connection-specific DNS Suffix . :
Description . . . . . : Intel(R) PRO/1000 MT Desktop Adapter
Physical Address. . . . . : 08-00-27-95-80-A7
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::739:399f:5c15:4ba1%7(Preferred)
IPv4 Address. . . . . : 192.168.10.100(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.10.1
DHCPv6 IAID . . . . . : 101187623
DHCPv6 Client DUID. . . . . : 00-01-00-01-2F-99-18-97-08-00-27-95-80-A7
DNS Servers . . . . . : 192.168.10.7
NetBIOS over Tcpip. . . . . : Enabled
C:\Users\DJ>


Computer Name/Domain Changes
Welcome to the decjag.dj domain.
OK
System
Comp
You c
compu
emote
computer
lary's
Computer name:
targetPC
Full computer name:
targetPC
More...
ork ID...
Member of
Domain:
decjag.dj
Workgroup:
WORKGROUP
nge...
OK
Cancel
OK
Cancel
Apply


Other user
User name
Password
Sign in to: DECJAG
How do I sign in to another domain?
DJ
Other user
ENG


Jenny Smith
Welcome