Installing
File and storage Manager
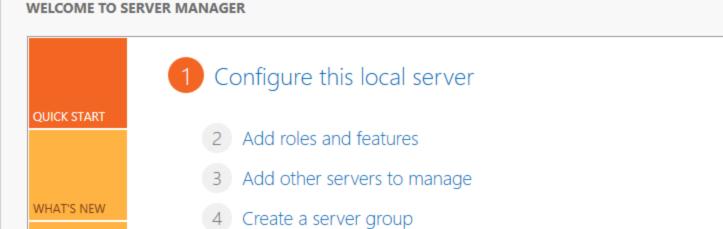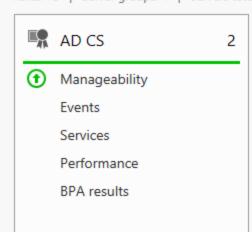
Server 2012

Server Manager ‣ Dashboard

Dashboard

Local Server

All Servers

AD CS

AD DS

AD FS

AD RMS

DHCP

DNS

File and Storage Services ▷

Finance Server Group

Hyper-V

IIS

IPAM ▷

mcsa group

NAP

Print Services

Remote Access

remotegroup

WDS

WSUS

WELCOME TO SERVER MANAGER

QUICK START

WHAT'S NEW

LEARN MORE

1 Configure this local server

2 Add roles and features

3 Add other servers to manage

4 Create a server group

ROLES AND SERVER GROUPS
Roles: 15 | Server groups: 4 | Servers total: 5

AD CS	2
⊕ Manageability	
Events	
Services	
Performance	
BPA results	

AD DS	2
⊕ Manageability	
Events	
Services	
Performance	
BPA results	

AD FS	
⊕ Manageability	
Events	
Services	
Performance	
BPA results	

Add Roles and Features Wizard

Before you begin

- 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

Add Roles and Features Wizard

Select installation type

Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results

Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD).

◉ **Role-based or feature-based installation**
   Configure a single server by adding roles, role services, and features.

○ **Remote Desktop Services installation**
   Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.

< Previous   Next >   Install   Cancel

Add Roles and Features Wizard

Select destination server

- Before You Begin
- Installation Type
- **Server Selection**
- Server Roles
- Features
- Confirmation
- Results

Select a server or a virtual hard disk on which to install roles and features.

- ◉ Select a server from the server pool
- ○ Select a virtual hard disk

Server Pool

Filter: _____

Name	IP Address	Operating System	
WIN-R44O8GIKKQK.Dea...	192.168.254.20...	Microsoft Windows Server 2012 Standard	

1 Computer(s) found

This page shows servers that are running Windows Server 2012, 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 >   Install   Cancel

Add Roles and Features Wizard

Select server roles

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

Roles

- ☑ Active Directory Certificate Services (Installed)
- ☑ Active Directory Domain Services (Installed)
- ▢ Active Directory Federation Services (Installed)
- ☐ Active Directory Lightweight Directory Services
- ▢ Active Directory Rights Management Services (Inst
- ☐ Application Server
- ☑ DHCP Server (Installed)
- ☑ DNS Server (Installed)
- ☐ Fax Server
- ☑ **File And Storage Services (Installed)**
  - ▢ File and iSCSI Services (Installed)
  - ☑ Storage Services (Installed)
- ☑ Hyper-V (Installed)
- ▢ Network Policy and Access Services (Installed)

Description

File and Storage Services includes services that are always installed, as well as functionality that you can install to help manage file servers and storage.

Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results

< Previous   Next >   Install   Cancel

Add Roles and Features Wizard

Select server roles

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

Roles

- ▷ ☐ Active Directory Rights Management Services (Inst
- ☐ Application Server
- ☑ DHCP Server (Installed)
- ☑ DNS Server (Installed)
- ☐ Fax Server
- ⊿ ☑ File And Storage Services (Installed)
  - ⊿ ☐ File and iSCSI Services (Installed)
    - ☑ File Server (Installed)
    - ☑ BranchCache for Network Files (Installed)
    - ☑ Data Deduplication (Installed)
    - ☑ DFS Namespaces (Installed)
    - ☑ DFS Replication (Installed)
    - ☑ File Server Resource Manager (Installed)
    - ☑ File Server VSS Agent Service (Installed)

Description

File Server Resource Manager helps you manage and understand the files and folders on a file server by scheduling file management tasks and storage reports, classifying files and folders, configuring folder quotas, and defining file screening policies.

< Previous   Next >   Install   Cancel

Manage **Tools** View

WELCOME TO SERVER MANAGER

- Dashboard
- Local Server
- All Servers
- AD CS
- AD DS
- AD FS
- AD RMS
- DHCP
- DNS
- File and Storage Services ▷
- Finance Server Group
- Hyper-V
- IIS
- IPAM ▷
- mcsa group
- NAP
- Print Services
- Remote Access
- remotegroup
- WDS

QUICK START

WHAT'S NEW

LEARN MORE

1 Configure this local server

2 Add roles and features

3 Add other servers to manage

4 Create a server group

ROLES AND SERVER GROUPS

Roles: 15 | Server groups: 4 | Servers total: 5

AD CS	2	AD DS	2	AD FS	2
⊕ Manageability		⊕ Manageability		⊕ Manageability	
Events		Events		Events	
Services		Services		Services	

Active Directory Administrative Center

Active Directory Domains and Trusts

Active Directory Module for Windows PowerShe

Active Directory Rights Management Services

Active Directory Sites and Services

Active Directory Users and Computers

AD FS Management

ADSI Edit

Certification Authority

Cluster-Aware Updating

Component Services

Computer Management

Connection Manager Administration Kit

Defragment and Optimize Drives

DFS Management

DHCP

Disk Cleanup

DNS

Event Viewer

Failover Cluster Manager

File Server Resource Manager

Group Policy Management

Health Registration Authority

Hyper-V Manager

Internet Information Services (IIS) Manager

File Server Resource Manager (Local)

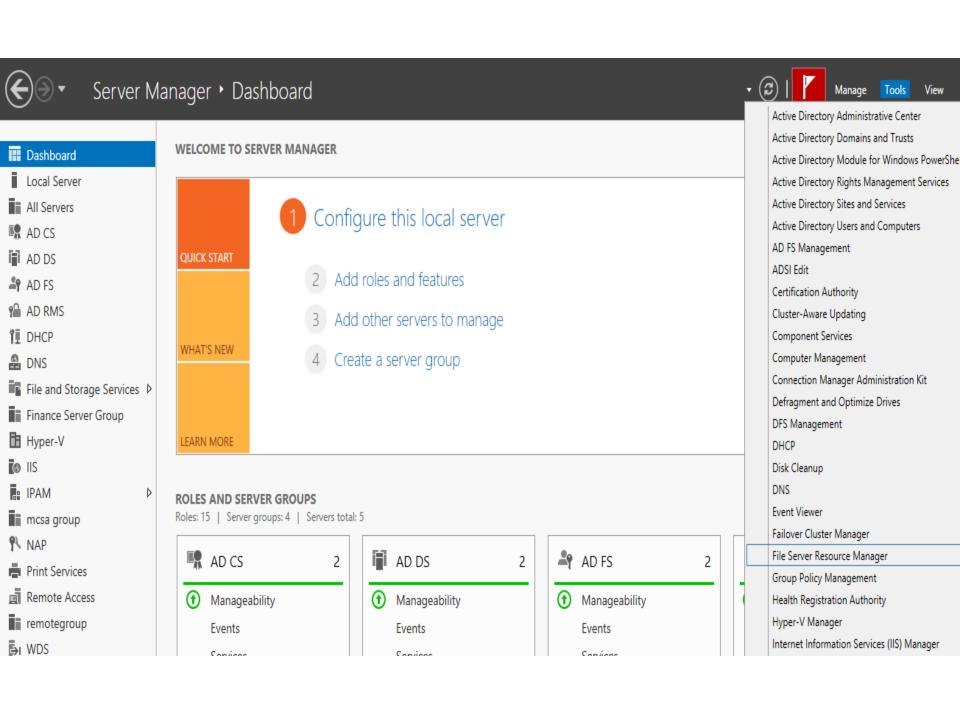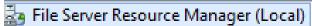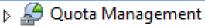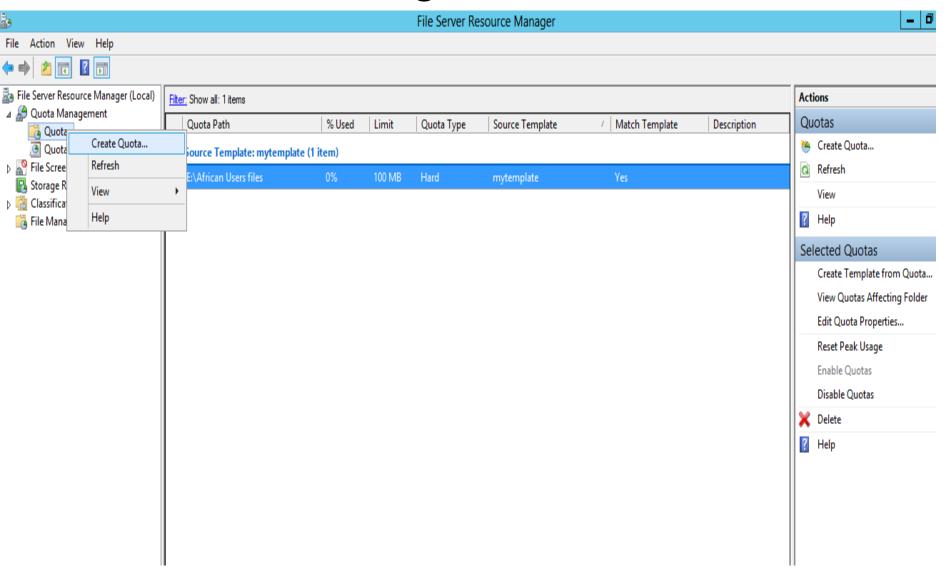| Name |
| --- |
| Quota Management |
| File Screening Management |
| Storage Reports Management |
| Classification Management |
| File Management Tasks |

Quota Management
File Screening Management
Storage Reports Management
Classification Management
File Management Tasks

Creating Quotas

Create Quota

Quota path:

E:\Finance1   [Browse...]

(•) Create quota on path

(○) Auto apply template and create quotas on existing and new subfolders

Quota properties

You can either use properties from a quota template or define custom quota properties.

How do you want to configure quota properties?

(•) Derive properties from this quota template (recommended):

    [100 MB Limit   ∨]

(○) Define custom quota properties

    [Custom Properties ...]

Summary of quota properties:

```
⊟ Quota: E:\Finance1
    ┈ Source template: 100 MB Limit
    ┈ Limit: 100 MB (Hard)
  ⊟ Notification: 4
      ┈ Warning(85%): Email
      ┈ Warning(95%): Email, Event log
```

[Create]   [Cancel]

Quota Properties of E:\Finance1 ✕

Copy properties from quota template (optional):

| 100 MB Limit ▾ | Copy |

Settings

Quota path:

E:\Finance1

Description (optional):

```

```

Space limit

Limit:

| 100.000 | MB ▾ |

◉ Hard quota: Do not allow users to exceed limit

○ Soft quota: Allow users to exceed limit (use for monitoring)

Notification thresholds

Threshold	E-mail	Event Log	Command	Report
Warning (85%)	✔			
Warning (95%)	✔	✔		
Warning (100%)	✔	✔		

| Add... | Edit... | Remove |

☐ Disable quota

| OK | Cancel |

Create file screen

File Server Resource Manager (Local)
- **Quota Management**
  - Quotas
  - Quota Templates
- **File Screening Management**
  - File Screens
  - File Screen Templates
  - File Groups
- **Storage Reports Management**
- **Classification Management**
- **File Management Tasks**

Filter: Show all: 1 items

File Screen Path	Screening Type	File Groups	Source Temp

Source Template: (1 item)

C:\filefolder

Create File Screen

File screen path:

`E:\African Users files` [Browse...]

File screen properties

You can either use properties from a file screen template or define custom file screen properties.

How do you want to configure file screen properties?

◉ Derive properties from this file screen template (recommended):

Block Audio and Video Files ▾

| Block Audio and Video Files |
| Block Executable Files |
| Block Image Files |
| Block E-mail Files |
| Monitor Executable and System Files |

○

Summary of file screen properties:

- File screen: E:\African Users files
  - Source template: Block Audio and Video Files
  - Screening type: Active
  - File groups: Audio and Video Files
  - Notifications: Email, Event log

[Create] [Cancel]

Create File Screen

File screen path:

E:\Finance2   [Browse...]

File screen properties

You can either use properties from a file screen template or define custom file screen properties.

How do you want to configure file screen properties?

○ Derive properties from this file screen template (recommended):

Block Audio and Video Files ▾

◉ Define custom file screen properties:

[Custom Properties ...]

Summary of file screen properties:

⊟ File screen: E:\Finance2
   ⋯ Screening type: Active
   ⋯ File groups:
   ⋯ Notifications:

[Create]   [Cancel]

File Screen Properties on E:\African Users files ✕

Copy properties from template (optional):

| Block Audio and Video Files ▾ | Copy |

Settings | E-mail Message | Event Log | Command | Report

File screen path:

E:\African Users files

Screening type:

⦿ Active screening: Do not allow users to save unauthorized files

◯ Passive screening: Allow users to save files (use for monitoring)

File groups

Select file groups to block:

- ☐ Audio and Video Files
- ☐ Backup Files
- ☐ Compressed Files
- ☐ E-mail Files
- ☐ Executable Files
- ☐ Image Files
- ☐ Office Files
- ☐ System Files

Maintain file groups:

| Create... |

| Edit... |

To select a file group to edit, highlight its label.

| OK | Cancel |

Editing the file group

File Group Properties for Image Files

Settings

File group name:

Image Files

To select a set of files, type a file name pattern, and click Add.
Examples: *.exe or Q4FY2002*.*

Files to include:

[Add] [Remove]

```
*.bmp
*.dib
*.eps
*.gif
*.img
*.jfif
```

Files to exclude:

[Add] [Remove]

[OK] [Cancel]

File Screen Properties on E:\Finance2 ✖

Copy properties from template (optional):

| Block Audio and Video Files | ⌄ | Copy |

Settings | **E-mail Message** | **Event Log** | **Command** | **Report**

☑ Send e-mail to the following administrators:

[Admin Email]

Format: account@domain. Use semicolons to separate accounts.

☐ Send e-mail to the user who attempted to save an unauthorized file

E-mail message

Type the text to use for the Subject line and message.

To identify the file screen, file group, user, or event associated with the current notification, you can use Insert Variable to insert a variable in your text

Subject:

Unauthorized file from the [Violated File Group] file group det

Message body:

User [Source Io Owner] attempted to save [Source File Path] to [File Screen Path] on the [Server] server. This file is in the [Violated File Group] file group, which is not permitted on the server.

Select variable to insert:

| [Admin Email] | ⌄ | Insert Variable |

Inserts the e-mail addresses of the administrators who receive the e-mail.

Additional E-mail Headers...

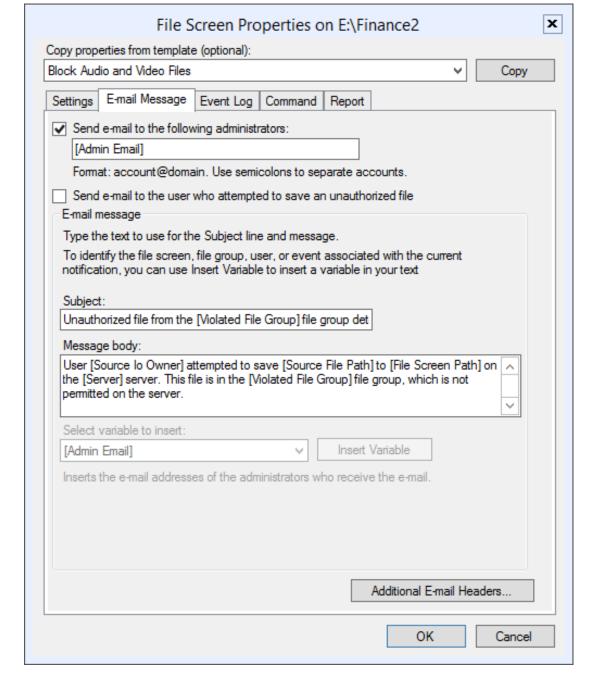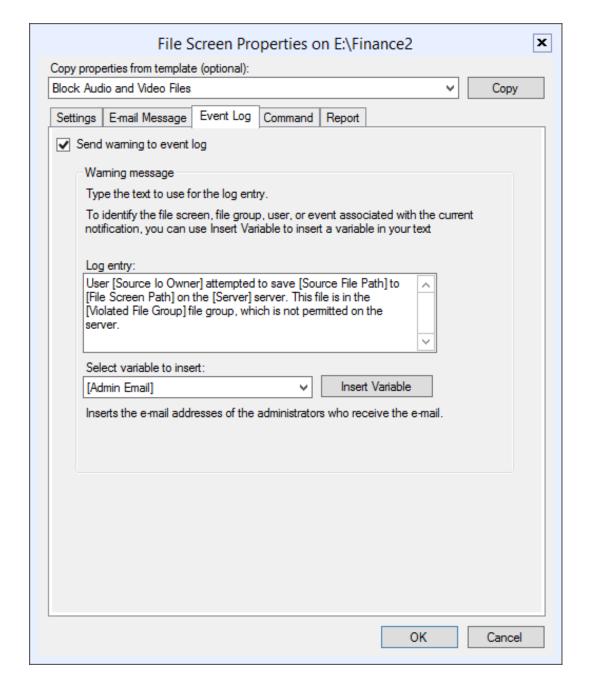OK | Cancel

File Screen Properties on E:\Finance2

Copy properties from template (optional):

Block Audio and Video Files | Copy

Settings | E-mail Message | **Event Log** | Command | Report

☑ Send warning to event log

Warning message

Type the text to use for the log entry.

To identify the file screen, file group, user, or event associated with the current notification, you can use Insert Variable to insert a variable in your text

Log entry:

User [Source Io Owner] attempted to save [Source File Path] to [File Screen Path] on the [Server] server. This file is in the [Violated File Group] file group, which is not permitted on the server.

Select variable to insert:

[Admin Email] | Insert Variable

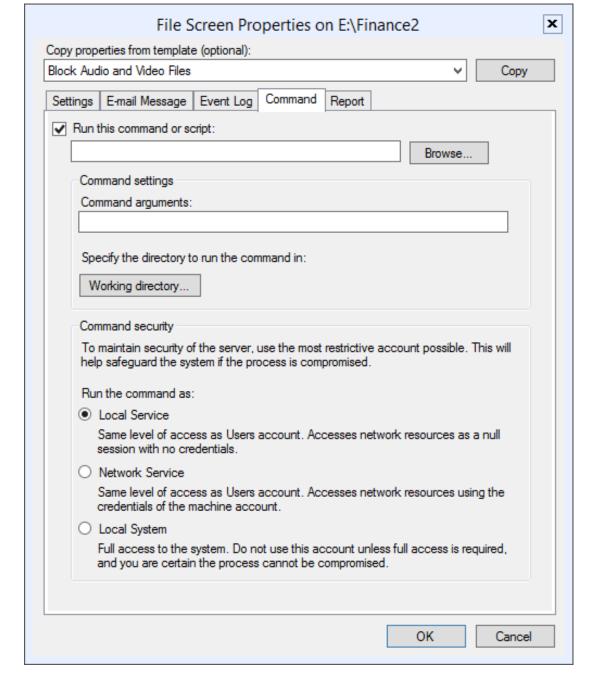Inserts the e-mail addresses of the administrators who receive the e-mail.

OK | Cancel

File Screen Properties on E:\Finance2 ✕

Copy properties from template (optional):

| Block Audio and Video Files ▼ | Copy |

| Settings | E-mail Message | Event Log | **Command** | Report |

☑ Run this command or script:

[   ] [Browse...]

Command settings

Command arguments:

[   ]

Specify the directory to run the command in:

[Working directory...]

Command security

To maintain security of the server, use the most restrictive account possible. This will help safeguard the system if the process is compromised.

Run the command as:

◉ Local Service

    Same level of access as Users account. Accesses network resources as a null session with no credentials.

◯ Network Service

    Same level of access as Users account. Accesses network resources using the credentials of the machine account.

◯ Local System

    Full access to the system. Do not use this account unless full access is required, and you are certain the process cannot be compromised.

[OK] [Cancel]

File Screen Properties on E:\Finance2 ✕

Copy properties from template (optional):

| Block Audio and Video Files | ▼ | Copy |

| Settings | E-mail Message | Event Log | Command | **Report** |

☑ Generate reports

Select reports to generate:

- ☐ Files by File Group
- ☐ Files by Owner
- ☐ Files by Property
- ☐ Large Files
- ☐ Least Recently Accessed Files
- ☐ Most Recently Accessed Files
- ☐ Quota Usage

[Review Selected Reports]

When a quota or file screening event generates incident reports, default report settings are used. To modify the default settings, use the Configure Options task, Storage Reports tab.

☐ Send reports to the following administrators:

[Admin Email]

Format: account@domain. Use a semicolon to separate multiple accounts.

☐ Send reports to the user who attempted to save an unauthorized file

The reports will be saved in E:\StorageReports\Incident.

To change the locations where reports are saved, use the Configure Options task, Report Locations tab.

[OK]   [Cancel]