Initial user installation consists of the following:

OptiPlex 3080 Small form factor
Dell 27” Monitor
Dell PowerEdge T440 Tower Server
16 Port Gigabit Ethernet POE Switch
Ubiquiti Networks Ap AC Pro Access Point POE
Bit defender Anti-Virus & Security Software
Windows 2019 Server Essentials

Vostro Desktop 3681
Dell 24 Monitor - S2421HN, 60.45 cm (23.8”), Free-Sync, HDMI cable
OptiPlex 7490 All-in-One BTX
Inspiron 15, 5510 Laptops (5)
Drake Tax Software has been installed on the server (Local drive mapping & Server Drive mapping)
Microsoft Office has been installed on all client Workstations (Desktops/Laptops)

All Desktops/laptops have the latest version of Windows 10, inclusive of security patches.

The client server room has been cleaned up according to the client’s directions.
All cabling is certified & tested CAT5.
An additional Gigabit Ethernet Switch has been installed in the middle of client's ceiling above the copier.

User accounts have been added to the server as follows:

Administrator Account Password is Cotton2021
Chris Watts
Roshanda Luter Rluter
Trever Edwards Tedwards
Payton Overstreet Poverstreet
Octavia Barnes Obarnes
Shavenne Stephenson Sstephenson
Dianna Brown Dbrown

A database product by Kintone has been set up in draft form. Client needs to determine a billing method for this option as client has stated they do not like to use ‘credit cards for this product.

The client has requested instructions on how to add user accounts.

Manage User Accounts in Windows Server Essentials

- Article
- 05/19/2022
- 27 minutes to read
- 8 contributors

Applies To: Windows Server 2016 Essentials, Windows Server 2012 R2 Essentials, Windows Server 2012 Essentials

The Users page of the Windows Server Essentials Dashboard centralizes information and tasks that help you manage the user accounts on your small business network. For an overview of the Users Dashboard, see Dashboard Overview.

Managing user accounts

The following topics provide information about how to use the Windows Server Essentials Dashboard to manage the user accounts on the server:

- Add a user account
- Remove a user account
- View user accounts
- Change the display name for the user account
- Activate a user account
- Deactivate a user account
- Understand user accounts
- Manage user accounts using the Dashboard

Add a user account

When you add a user account, the assigned user can log on to the network, and you can give the user permission to access network resources such as shared folders and the Remote Web Access site. Windows Server Essentials includes the Add a User Account Wizard that helps you:

- Provide a name and password for the user account.
- Define the account as either an administrator or as a standard user.
- Select which shared folders the user account can access.
- Specify if the user account has remote access to the network.
- Select email options if applicable.
- Assign a Microsoft Online Services account (referred to as a Microsoft 365 account in Windows Server Essentials) if applicable.
- Assign user groups (Windows Server Essentials only).

Note

- Non-ASCII characters are not supported in Microsoft Azure Active Directory (Azure AD). Do not use any non-ASCII characters in your password, if your server is integrated with Azure AD.
    - The email options are only available if you install an add-in that provides email service.

To add a user account

1. Open the Windows Server Essentials Dashboard.
2. On the navigation bar, click **Users**.
3. In the **Users Tasks** pane, click **Add a user account**. The Add a User Account Wizard appears.
4. Follow the instructions to complete the wizard.

Remove a user account

When you choose to remove a user account from the server, a wizard deletes the selected account. Because of this, you can no longer use the account to log on to the network or to access any of the network resources. As an option, you can also delete the files for the user account at the same time that you remove the account. If you do not want to permanently remove the user account, you can deactivate the user account instead to suspend access to network resources.

Important

If a user account has a Microsoft online account assigned, when you remove the user account, the online account also is removed from Microsoft Online Services, and the user's data, including email, is subject to data retention policies in Microsoft Online Services. If you want to retain user data for the online account, deactivate the user account instead of removing it. For more information, see **Manage Online Accounts for Users**.

To remove a user account

5. Open the Windows Server Essentials Dashboard.
6. On the navigation bar, click **Users**.
7. In the list of user accounts, select the user account that you want to remove.
8. In the **<User Account> Tasks** pane, click **Remove the user account**. The Delete a User Account Wizard appears.
9. On the **Do you want to keep the files?** page of the wizard, you can choose to delete the user's files, including File History backups and the redirected folder for the user account. To keep the user's files, leave the check box empty. After making your selection, click **Next**.
10. Click **Delete account**.

Note

After you remove a user account, the account no longer appears in the list of user accounts. If you chose to delete the files, the server permanently deletes the user's folder from the **Users** server folder and from the **File History Backups** server folder.

If you have an integrated email provider, the email account assigned to the user account will also be removed.

View user accounts

The **Users** section of the Windows Server Essentials Dashboard displays a list of network user accounts. The list also provides additional information about each account.

To view a list of user accounts

11. Open the Windows Server Essentials Dashboard.
12. On the main navigation bar, click **Users**.
13. The Dashboard displays a current list of user accounts.

To view or change properties for a user account

14. In the list of user accounts, select the account for which you want to view or change properties.

15. In the **<User Account> Tasks** pane, click **View the account properties**. The **Properties** page for the user account appears.
16. Click a tab to display the properties for that account feature.
17. To save any changes that you make to the user account properties, click **Apply**.

Change the display name for the user account

The display name is the name that appears in the **Name** column on the **Users** page of the Dashboard. Changing the display name does not change the logon or sign-in name for a user account.

To change the display name for a user account

18. Open the Windows Server Essentials Dashboard.
19. On the navigation bar, click **Users**.
20. In the list of user accounts, select the user account that you want to change.
21. In the **<User Account> Tasks** pane, click **View the account properties**. The **Properties** page for the user account appears.
22. On the **General** tab, type a new **First name** and **Last name** for the user account, and then click **OK**.
23. The new display name appears in the list of user accounts.

Activate a user account

When you activate a user account, the assigned user can log on to the network and access network resources to which the account has permission, such as shared folders and the Remote Web Access site.

Note

You can only activate a user account that is deactivated. You cannot activate a user account after you remove it from the server.

To activate a user account

24. Open the Windows Server Essentials Dashboard.
25. On the navigation bar, click **Users**.
26. In the list view, select the user account that you want to activate.
27. In the **<User Account> Tasks** pane, click **Activate the user account**.
28. In the confirmation window, click **Yes** to confirm your action.

Note

After you activate a user account, the status for the account displays **Active**. The user account regains the same access rights that were assigned prior to account deactivation.

If you have an integrated email provider, the email account assigned to the user account will also be activated.

Deactivate a user account

When you deactivate a user account, account access to the server is temporarily suspended. Because of this, the assigned user cannot use the account to access network resources such as shared folders or the Remote Web Access site until you activate the account.

If the user account has a Microsoft online account assigned, the online account is also deactivated. The user cannot use resources in Microsoft 365 and other online services that you subscribe to, but the user's data, including email, is retained in Microsoft Online Services.

Note

You can only deactivate a user account that is currently active.

To deactivate a user account

29. Open the Windows Server Essentials Dashboard.
30. On the navigation bar, click **Users**.
31. In the list view, select the user account that you want to deactivate.
32. In the **<User Account> Tasks** pane, click **Deactivate the user account**.
33. In the confirmation window, click **Yes** to confirm your action.

Note

After you deactivate a user account, the status for the account displays **Inactive**.

If you have an integrated email provider, the email account assigned to the user account will also be deactivated.

Understand user accounts

A user account provides important information to Windows Server Essentials, which enables individuals to access information that is stored on the server, and makes it possible for individual users to create and manage their files and settings. Users can log on to any computer on the network if they have a Windows Server Essentials user account and they have permissions to access a computer. Users access their user accounts with their user name and password.

There are two main types of user accounts. Each type gives users a different level of control over the computer:

- **Standard** accounts are for everyday computing. The standard account helps protect your network by preventing users from making changes that affect other users, such as deleting files or changing network settings.
- **Administrator** accounts provide the most control over a computer network. You should assign the administrator account type only when necessary.

Manage user accounts using the Dashboard

Windows Server Essentials makes it possible to perform common administrative tasks by using the Windows Server Essentials Dashboard. By default, the **Users** page of the Dashboard includes two tabs: **Users** and **Users Groups**.

Note

- If you integrate your server that is running Windows Server Essentials with Microsoft 365, a new tab called **Distribution Groups** is also added within the **Users** page of the Dashboard.
    - In Windows Server Essentials, the **Users** page of the Dashboard includes only a single tab - **Users**.

The **Users** tab includes the following:

- A list of user accounts, which displays:
    - The name of the user.
    - The Logon name for the user account.
    - Whether the user account has Anywhere Access permission. Anywhere Access permission for a user account is either **Allowed** or **Not allowed**.
    - Whether the File History for this user account is managed by the server running Windows Server Essentials. The File History status for a user account is either **Managed** or **Not managed**.
    - The level of access that is assigned to the user account. You can assign either **Standard user** access or **Administrator** access for a user account.
    - The user account status. A user account can be **Active**, **Inactive**, or **Incomplete**.
    - In Windows Server Essentials, if the server is integrated with Microsoft 365 or Windows Intune, the Microsoft online account is displayed.
    - In Windows Server Essentials, if the server is integrated with Microsoft 365, the status of the account (known in Windows Server Essentials as the Microsoft online account) for the user account is displayed.
- A details pane with additional information about a selected user account.
- A tasks pane that includes:
    - A set of user account administrative tasks such as viewing and removing user accounts, and changing passwords.
    - Tasks that allow you to globally set or change settings for all user accounts in the network.

- The following table describes the various user account tasks that are available from the **Users** tab. Some of the tasks are user account-specific, and they are only visible when you select a user account in the list.

Note

If you integrate Microsoft 365 with Windows Server Essentials, additional tasks will become available. For more information, see **Manage Online Accounts for Users**.

User account tasks in the Dashboard

Task name	Description
View the account properties	Enables you to view and change the properties of the selected user account, and to specify folder access permissions for the account.
Deactivate the user account	A user account that is deactivated cannot log on to the network or access network resources such as shared folders or printers.
Activate the user account	A user account that is activated can log on to the network and can access network resources as defined by the account permissions.
Remove the user account	Enables you to remove the selected user account.

Change the user account password	Enables you to reset the network password for the selected user account.
Add a user account	Starts the Add a User Account Wizard, which enables you to create a single new user account that has either standard user access or administrator access.
Assign a Microsoft online account	Adds a Microsoft online account to the local network user account that is selected. This task is displayed when your server is integrated with Microsoft online services, such as Microsoft 365.
Add Microsoft online accounts	Adds Microsoft online accounts and associates them to local network user accounts. This task is displayed when your server is integrated with Microsoft online services, such as Microsoft 365.
Set the password policy	Enables you to change the values of the password polices for your network.
Import Microsoft online accounts	Performs a bulk import of accounts from Microsoft online services into the local network. This task is displayed when your server is integrated with Microsoft online services, such as Microsoft 365.
Refresh	Refreshes the Users tab. This task is applicable to Windows Server Essentials.
Change File History settings	Enables you to change File History settings, such as backup frequency, or backup duration. This task is applicable to Windows Server Essentials.
Export all remote connections	Creates a .CSV-format file of all remote connections to the server that have occurred over the past 30 days.

Managing passwords and access

The following topics provide information about how to use the Windows Server Essentials Dashboard to manage user account passwords and user access to the shared folders on the server:

- Change or reset the password for a user account
- What you should know about password policies
- Change the password policy
- Level of access to shared folders
- Retain and manage access to files for removed user accounts
- Synchronize the DSRM password with the network administrator password
- Give user accounts remote desktop permission

- Enable users to access resources on the server
- Change remote access permissions for a user account
- Change virtual private network permissions for a user account
- Change access to internal shared folders for a user account
- Allow user accounts to establish a remote desktop session to their computer

Change or reset the password for a user account
To change or reset a user account password, follow these steps.

To reset the password for a user account

34. Open the Windows Server Essentials Dashboard.
35. On the navigation bar, click **Users**.
36. In the list of user accounts, select the user account that you want to reset.
37. In the **<User Account> Tasks** pane, click **Change the user account password**. The Change User Account Password Wizard appears.
38. Type a new password for the user account, and then type the password again to confirm it.
39. Click **Change password**.
40. Provide the new password to the user.

41. **Important**

    - You may not be able to change your password if the password policy for your account has been set to **Passwords never expire**.
        - Non-ASCII characters are not supported in Azure AD. Therefore, if your server is integrated with Azure AD, do not use any non-ASCII characters in your password.
        - If a Microsoft online account (known in Windows Server Essentials as a Microsoft 365 account) is assigned to the user, the password is synchronized with the online account password. The user will use the new password to sign in on the server or sign in to Microsoft 365. For more information, see **Manage Online Accounts for Users**.

What you should know about password policies
The password policy is a set of rules that define how users create and use passwords. The policy helps to prevent unauthorized access to user data and other information that is stored on the server. The password policy is applied to all user accounts that access the network.

The Windows Server Essentials password policy consists of three primary elements as follows:

- **Password length**. The longer a password is, the more secure it is. Blank passwords are not secure.
- **Password complexity**. Complex passwords contain a mixture of uppercase and lowercase letters (a-z, A-Z), base numbers (0-9), and non-alphabetic symbols (such as; !,@,#,_,-). Complex passwords are much less susceptible to unauthorized access. Passwords that contain user names, birthdates, or other personal information do not provide adequate security.

- **Password age**. Windows Server Essentials requires that users change their password at least once every 180 days. As an option, you can choose to have passwords never expire.
- To make it easier to implement a password policy on your computer network, Windows Server Essentials provides a simple tool that allows you to set or change the password policy to any of the following four pre-defined policy profiles:
- **Weak**. Users can specify any password that is not blank.
- **Medium**. These passwords must contain at least 5 characters. A complex password is not required.
- **Medium Strong**. These passwords must contain at least 5 characters, and must include letters, numbers, and symbols.
- **Strong**. These passwords must contain at least 7 characters, and must include letters, numbers, and symbols. These passwords are more secure, but may be more difficult for users to remember.
- **Note**
- Passwords cannot contain the user name or email address.
- If you integrate with Microsoft 365, the integration enforces the **Strong** password policy, and updates the policy to include the following requirements:
    - Passwords must contain 8 ?16 characters.
        - Passwords cannot contain a space or the Microsoft 365 email name.
- By default, server installation sets the default password policy to the **Strong** option.

Change the password policy

Use the following procedure to set or change the password policy to any of four pre-defined policy profiles.

To change the password policy

42. Open the Windows Server Essentials Dashboard, and then click **Users**.
43. In the **Users Tasks** pane, click **Set the password policy**.
44. On the **Change the Password Policy** screen, set the level of password strength by moving the slider.
45. Microsoft recommends that you set the password strength to **Strong**.
46. **Note**
47. As an option, you can also select **Passwords never expire**. This setting is less secure, and so it is not recommended.
48. Click **Change policy**.

Level of access to shared folders

As a best practice, you should assign the most restrictive permissions available that still allow users to perform required tasks.

You have three access settings available for the shared folders on the server:

- **Read/Write**. Choose this setting if you want to allow the user account permission to create, change, and delete any files in the shared folder.
- **Read only**. Choose this setting if you want to allow the user account permission to only read the files in the shared folder. User accounts with read-only access cannot create, change, or delete any files in the shared folder.
- **No access**. Choose this setting if you do not want the user account to access any files in the shared folder.

Retain and manage access to files for removed user accounts

The network administrator can remove a user account and choose to keep the user's files for future use. In this scenario, the removed user account can no longer be used to sign in to the network; however, the files for this user will be saved in a shared folder, which can be shared with another user.

Important

Be aware that if you remove a user account that has a Microsoft online account assigned, the online account is also removed, and the user data, including email, is subject to data retention policies in Microsoft Online Services. To retain the user data for the online account, deactivate the user account instead of removing it. For more information, see **Manage Online Accounts for Users**.

To remove a user account but retain access to the user's files

49. Open the Windows Server Essentials Dashboard.
50. On the navigation bar, click **Users**.
51. In the list of user accounts, select the user account that you want to remove.
52. In the **<User Account> Tasks** pane, click **Remove the user account**. The Delete a User Account Wizard appears.
53. On the **Do you want to keep the files?** page, make sure that the **Delete the files including File History backups and redirected folder for this user account** check box is clear, and then click **Next**.
54. A confirmation page appears warning you that are deleting the account but keeping the files.
55. Click **Delete account** to remove the user account.
56. After the user account is removed, the administrator can give another user account access to the shared folder.

To give a user account permission to access a shared folder

57. Open the Windows Server Essentials Dashboard.
58. On the navigation bar, click **Storage**, and then click the **Server Folders** tab.
59. In the list of folders, select the **Users** folder.
60. In the **Users Tasks** pane, click **Open the folder**. Windows Explorer opens and displays the contents of the **Users** folder.

61. Right-click the folder for the user account that you want to share, and then click **Properties**.
62. In **<User Account> Properties**, click the **Sharing** tab, and then click **Share**.
63. In the **File Sharing** window, type or select the user account name with whom you want to share the folder, and then click **Add**.
64. Choose the **Permission Level** that you want the user account to have, and then click **Share**.

Synchronize the DSRM password with the network administrator password

Directory Services Restore Mode (DSRM) is a special boot mode for repairing or recovering Active Directory. The operating system uses DSRM to log on to the computer if Active Directory fails or needs to be restored. If your network administrator password and the DSRM password are different, DSRM will not load.

During a clean, first-time installation of Windows Server Essentials, the program sets the DSRM password to the network administrator account password that you specify during setup or in the migration answer file. When you change your network administrator password (as recommended typically every 60 days for increased server security), the password change is not forwarded to DSRM. This results in a password mismatch. If this occurs, you can use the following solutions to manually or automatically synchronize your network administrator's password with the DSRM password.

To manually synchronize the DSRM password to a network administrator account

65. At a command prompt, run ntdsutil.exe to open the ntdsutil tool.
66. To reset the DSRM password, type **set dsrm password**.
67. To synchronize the DSRM password on a domain controller with the current network administrator's account, type:

68. **sync from domain account** <*current_network_administrator_account*>, and then press Enter.

69. Because you will periodically change the password for the network administrator account, to ensure that the DSRM password is always the same as the current password of the network administrator, we recommend that you create a schedule task to automatically synchronize the DSRM password to the network administrator password daily.

To automatically synchronize the DSRM password to a network administrator account

70. From the server, open **Administrative Tools**, and then double-click **Task Scheduler**.
71. In the Task Scheduler **Actions** pane, click **Create Task**.
72. In the **Name** text box, type a name for the task such as **AutoSync DSRM Password**, and then select the **Run with highest privileges** option.
73. Define when the task should run:
    a. In the **Create Task** dialog box, click the **Triggers** tab, and then click **New**.
    b. In the **New Trigger** dialog box, select your recurrence option, specify the recurrence interval, and choose a start time.

    c. Note

d. As a best practice, you should set the task to run daily during non-business hours.

e. Click **OK** to save your changes and return to the **Create Task** dialog box.

74. Define the task actions:
    f. Click the **Actions** tab, and then click **New**. The **New Action** dialog box appears.
    g. In the **Action** list, click **Start a program**, and then browse to **C:\WINDOWS\SYSTEM32\ntdsutil.exe**.
    h. In the **Add arguments**(optional) text box, type the following (you must include the quotation marks): **set dsrm password sync from domain account SBS_network_administrator_account q q** where *SBS_network_administrator_account* is the current network administrator's account name.
75. Click **OK** twice to save the task and close the **Create Task** dialog box. The new task appears in the **Active Tasks** section of **Task Schedule**.

Give user accounts remote desktop permission

In the default installation of Windows Server Essentials, network users do not have permission to establish a remote connection to computers or other resources on the network.

Before network users can establish a remote connection to network resources, you must first set up Anywhere Access. After you set up Anywhere Access, users can access files, applications, and computers in your office network from a device in any location with an Internet connection.

The Set up Anywhere Access Wizard allows you to enable two methods of remote access:

- Virtual private network (VPN)
- Remote Web Access

- When you run the wizard, you can also choose to allow Anywhere Access for all current and newly added user accounts.

- To set up Anywhere Access, open the Dashboard **Home** page, click **SETUP**, and then click **Set up Anywhere Access**.

- For more information about Anywhere Access, see Manage Anywhere Access.

Enable users to access resources on the server

This section applies to a server running Windows Server Essentials or Windows Server Essentials, or to a server running Windows Server 2012 R2 Standard or Windows Server 2012 R2 Datacenter with the Windows Server Essentials Experience role installed.

If you want users to use remote access, and/or have individual user accounts, after you finish connecting a computer to the server, you can create new network user accounts for the users of the networked computer on the server by using the Dashboard. For more information about creating a user account, see Add a user account. After creating the user accounts, you must provide the network user name and password information to the users of the client computer so that they can access resources on the server by using the Launchpad.

For each user account that you create you can set access for the following through the user account properties:

- **Shared folders**. By default, network administrators have **Read/Write** permission to all the shared folders, and standard user accounts have **Read-only** permissions to the Company folder. If media streaming is enabled, you can assign folder access permissions for individual standard user accounts for the following shared folders: **Music**, **Pictures**, **Recorded TV**, and **Videos**. You can set permissions for user accounts to access shared folders on the **Shared folders** tab of the user account properties.
- **Anywhere Access**. By default, network administrators can use either VPN or Remote Web Access to access server resources. For standard user accounts, you must set user account permissions on the **Anywhere Access** tab.
- **Computer access**. By default, network administrators can access all the computers in the network. However, for standard user accounts you can set individual user account permissions for accessing computers on the network on the **Computer access** tab of the user account properties.

To edit user account properties in Windows Server Essentials 2012 R2

76. Open the Windows Server Essentials Dashboard.
77. On the navigation bar, click **USERS**.
78. In the list of user accounts, select the user account that you want to edit.
79. In the **<User Account> Tasks** pane, click **View the account properties**.
80. In the **<User Account> Properties**, do the following:
    i. On the **Shared folders** tab, set the appropriate folder permissions for each shared folder as needed.
    j. On the **Anywhere Access** tab:
        i. To allow a user to connect to the server by using VPN, select the **Allow Virtual Private Network (VPN)** check box.
        ii. To allow a user to connect to the server by using Remote Web Access, select the **Allow Remote Web Access and access to web services applications** check box.
    k. On the **Computer access** tab, select the network computers that you would like the user to have access to.