BitLocker: How to deploy on Windows Server 2012

4 out of 5 rated this helpful - Rate this topic

Published: August 30, 2012

Updated: August 30, 2012

Applies To: Windows Server 2012

For all Windows Server editions, BitLocker must be installed using Server Manager. However, you can still provision BitLocker before the server operating system is installed as part of your deployment.

Installing BitLocker

BitLocker requires administrator privileges on the server to install. You can install BitLocker either by using Server Manager or Windows PowerShell cmdlets.

- To install BitLocker using Server Manager
- To install BitLocker using Windows PowerShell

To install BitLocker using Server Manager

1. Open Server Manager by selecting the Server Manager icon or running servermanager.exe.
2. Select **Manage** from the **Server Manager Navigation** bar and select **Add Roles and Features** to start the **Add Roles and Features Wizard.**
3. With the **Add Roles and Features Wizard** open, select **Next** at the **Before you begin** pane (if shown).
4. Select **Role-based or feature-based installation** on the **Installation type** pane of the **Add Roles and Features Wizard** pane and select **Next** to continue.
5. Select the **Select a server from the server pool option** in the **Server Selection** pane and confirm the server for the BitLocker feature install.

6. Server roles and features install using the same wizard in Server Manager. Select **Next** on the **Server Roles** pane of the **Add Roles and Features** wizard to proceed to the **Features** pane.

7. Select the check box next to **BitLocker Drive Encryption** within the **Features** pane of the **Add Roles and Features Wizard**. The wizard will show the additional management features available for BitLocker. If you do not want to install these features, deselect the **Include management tools option** and select **Add Features**. Once optional features selection is complete, select **Next** to proceed in the wizard.

   Note

   The **Enhanced Storage** feature is a required feature for enabling BitLocker. This feature enables support for Encrypted Hard Drives on capable systems. For more information on Encrypted Hard Drive support, please see Encrypted Hard Drive.

8. Select **Install** on the **Confirmation** pane of the **Add Roles and Features Wizard** to begin BitLocker feature installation. The BitLocker feature requires a restart to complete. Selecting the **Restart the destination server automatically if required** option in the **Confirmation** pane will force a restart of the computer after installation is complete.

9. If the **Restart the destination server automatically if required** check box is not selected, the **Results pane** of the **Add Roles and Features Wizard** will display the success or failure of the BitLocker feature installation. If required, a notification of additional action necessary to complete the feature installation, such as the restart of the computer, will be displayed in the results text.

To install BitLocker using Windows PowerShell

Windows PowerShell offers administrators another option for BitLocker feature installation. Windows PowerShell installs features using the `servermanager` or `dism` module; however, the `servermanager` and `dism` modules do not always share feature name parity. Because of this, it is advisable to confirm the feature or role name prior to installation.

Note

The BitLocker feature requires the server to be restarted after installation to fully install.

Using the servermanager module to install BitLocker

The `servermanager` Windows PowerShell module can use either the `Install-WindowsFeature` or `Add-WindowsFeature` to install the BitLocker feature. The `Add-WindowsFeature` cmdlet is merely a stub to the `Install-WindowsFeature`. This example uses the `Install-WindowsFeature` cmdlet. The feature name for BitLocker in the `servermanager` module is `BitLocker`. This can be determined using the `Get-WindowsFeature` cmdlet with a query such as:

```
Get-WindowsFeature Bit
```

The results of this command displays a table of all of the feature names beginning with "Bit" as their prefix. This allows you to confirm that the feature name is `BitLocker` for the BitLocker feature.

By default, installation of features in Windows PowerShell does not include optional sub-features or management tools as part of the install process. This can be seen using the `-WhatIf` option in Windows PowerShell.

```
Install-WindowsFeature BitLocker -WhatIf
```

The results of this command show that only the BitLocker Drive Encryption feature installs using this command.

To see what would be installed with the BitLocker feature including all available management tools and sub-features, use the following command:

```
Install-WindowsFeature BitLocker -IncludeAllSubFeature -
IncludeManagementTools -WhatIf | fl
```

The result of this command displays the following list of all the administration tools for BitLocker that would be installed along with the feature, including tools for use with Active Directory Domain Services (AD DS) and Active Directory Lightweight Directory Services (AD LDS).

- BitLocker Drive Encryption
- BitLocker Drive Encryption Tools
- BitLocker Drive Encryption Administration Utilities
- BitLocker Recovery Password Viewer
- AD DS Snap-Ins and Command-Line Tools
- AD DS Tools
- AD DS and AD LDS Tools

The command to complete a full installation of the BitLocker feature with all available features and then rebooting the server at completion is:

```
Install-WindowsFeature BitLocker -IncludeAllSubFeature -
IncludeManagementTools -Restart
```

Important

Installing the BitLocker feature using Windows PowerShell does not install the Enhanced Storage feature. Administrators wishing to support Encrypted Hard Drives in their environment will need to install the Enhanced Storage feature separately.

Using the dism module to install BitLocker

The `dism` Windows PowerShell module uses the `Enable-WindowsOptionalFeature` cmdlet to install features. The BitLocker feature name for BitLocker is `BitLocker`. The `dism` module does not support wildcards when searching for feature names. To list feature names for the `dism` module, use the `Get-WindowsOptionalFeatures` cmdlet. The following command will list all of the optional features in an online (running) operating system.

```
Get-WindowsOptionalFeature -Online | ft
```

From this output, we can see that there are three BitLocker related optional feature names: BitLocker, BitLocker-Utilities and BitLocker-NetworkUnlock. To install the BitLocker feature, the BitLocker and BitLocker-Utilities features are the only required items.

To install BitLocker using the `dism` module, use the following command:

```
Enable-WindowsOptionalFeature -Online -FeatureName BitLocker -All
```

This command will prompt the user for a reboot. The Enable-WindowsOptionalFeature cmdlet does not offer support for forcing a reboot of the computer. This command does not include installation of the management tools for BitLocker. For a complete installation of BitLocker and all available management tools, use the following command:

```
Enable-WindowsOptionalFeature -Online -FeatureName BitLocker, BitLocker-
Utilities -All
```